

MISRA SC

Vehicle Lifecycle Safety Assurance Argument for Automated Driving

June 2026



First published April 2026 by The MISRA Consortium Limited
1 St James Court
Whitefriars
Norwich
Norfolk
NR3 1RU
UK

www.misra.org.uk

Copyright © The MISRA Consortium Limited 2026.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or photocopying, recording or otherwise without the prior written permission of the Publisher.

“MISRA”, “MISRA C” and the triangle logo are registered trademarks owned by The MISRA Consortium Ltd.

Other product or brand names are trademarks or registered trademarks of their respective holders and no endorsement or recommendation of these products by MISRA is implied.

ISBN 978-1-911700-28-9 PDF

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

MISRA Mission Statement

We provide world-leading best practice guidelines for the safe and secure application of both embedded control systems and standalone software.

MISRA is a collaboration between manufacturers, component suppliers, engineering consultancies and academics which seeks to research and promote best practice in developing safety- and security-related electronic systems and other software-intensive applications.

To this end MISRA conducts research projects and publishes documents that provide accessible information for engineers and management.

MISRA also facilitates the dissemination and exchange of information between practitioners through supporting and holding technical events.

Disclaimer

Compliance with the requirements of this document, or any other standard, does not of itself confer immunity from legal obligations.

Acknowledgements

The MISRA SC Working Group

The MISRA Consortium would like to thank the following individuals for their significant contribution to the writing of this document:

David Blackburn	Rimac Technology
Helen Monkhouse	HORIBA MIRA Ltd
Roger Rivett	Independent Functional Safety Specialist

The MISRA Consortium also wishes to acknowledge contributions from the following individuals to the development and review process:

David Ward	John Botham

Other acknowledgements

This document was typeset using Open Sans. Copyright 2020, The Open Sans Project Authors. Licensed under the SIL Open Font License, 1.1.

Contents

1 Background 1

2 Introduction 2

2.1 Previous white papers 2
2.2 Product Entity Ontology 3
2.3 Vehicle Lifecycle Claims 4

3 Vehicle context 8

3.1 Vehicle architecture 8
3.2 Vehicle control authority 9
3.3 Vehicle Safety 9

4 Mitigation of harm in lifecycle phases 10

4.1 Development 10
4.1.1 Safety Issues 10
4.1.2 Development phase mitigation 10
4.1.3 E/E System Support for Other Phases 10
4.2 Manufacturing 11
4.2.1 Safety Issues 11
4.2.2 Manufacturing phase mitigation 11
4.2.3 Development phase mitigation 12
4.3 Pre-ownership 12
4.3.1 Safety issues 12
4.3.2 Pre-ownership phase mitigation 13
4.3.3 Development phase mitigation 13
4.4 Pre-journey 13
4.4.1 Safety issues 13
4.4.2 Pre-journey phase mitigations 14
4.4.3 Development phase mitigations 16
4.5 During journey 17
4.5.1 Safety Issues 17
4.5.2 Journey phase mitigations 18
4.5.3 Development phase mitigations 19
4.6 Post-journey 20
4.6.1 Safety issues 20
4.6.2 Post-journey phase mitigation 21
4.6.3 Development phase mitigation 22
4.7 Maintenance & Repair 23
4.7.1 Safety issues 23
4.7.2 Maintenance & Repair phase mitigation 23

4.7.3 Development phase mitigation 24
4.8 Decommissioning 24
4.8.1 Safety issues 24
4.8.2 Decommissioning phase mitigation 25
4.8.3 Development phase mitigation 25

5 During Journey GSN Argument 26

5.1 Overall context 26
5.2 ADS during journey context 27
5.3 Teleoperation Team example 28
5.3.1 Harm identification 28
5.3.2 Harm mechanisms 29
5.3.3 Dur-j_1During Journey Phase Mitigation 30
5.3.4 Dur-j_Oth_1Development Phase Mitigation 31
5.3.5 Assumptions 31
5.4 ADS example 31
5.4.1 Harm identification 31
5.4.2 Harm mechanisms 32
5.4.3 Dur-j_1During Journey Phase Mitigation 33
5.4.4 Dur-j_Oth_1 Development Phase Mitigation 34
5.4.5 Assumptions 36

6 Summary of responsibility transfer from human to ADS vehicle control authority 37

7 Summary of Work to Date 38

8 Annex A - Examples by lifecycle phase 41

8.1 Development phase example 41
8.2 Manufacturing example 42
8.3 Pre-ownership example 42
8.4 Pre-journey example 43
8.5 During journey example 44
8.6 Post journey example 45
8.7 Maintenance & repair example 47
8.8 Decommissioning example 48

9 Annex B - Typical Topics to Support Development Claims 50

10 Terminology 57

11 References 58

12 Revision history 59

1 Background

The MISRA Safety Case working group published the *Guidelines for Automotive Safety Arguments* (GASA) [1] in September 2019. This document restricted its scope to the safety case argument required by ISO 26262 *Road vehicles — Functional safety* [2]. Since 2019, the working group has been responding to the automotive industry's work to produce vehicles with high and full driving automation. Our focus is safety which means the scope of this document is the prevention of harm to people. The aspiration of the group is to understand what will be necessary to produce a safety assurance argument for vehicles with high and full driving automation (i.e. SAE Levels 4 and 5 [14]).

In 2020 the working group published *A Structured Argument for Assuring Safety of the Intended Functionality (SOTIF)* [3], which introduced the concept of the 4-state model. This model is intended to help reason about completeness when defining behaviour in the context of SOTIF [11]. In 2022, Roger Rivett published *Public Road Transport and Vehicle Models* [4], which presents an ontology[1] of the whole public road transport system. This includes the physical road network and supporting infrastructure, the weather, users of the road network and their interactions with the external environment.

In April 2024, MISRA SC published the white paper *Safety Assurance Argument Context for Automated Driving* [6], also referred to as White Paper 1. This white paper provided an overall context within which a safety assurance argument for a vehicle with high or full driving automation has to be made. The white paper consisted of two potential contexts for driving automation. The first was personal transport viewed as a service, in which an Automated Driving System (ADS) equipped vehicle [5] would participate. This view includes all the aspects that contribute to the overall service. The second context addressed the complete vehicle lifecycle from development, through operation and maintenance, to decommissioning.

For both contexts, an ontology of the terms used in the subject matter was presented, and also a claim structure to show how a safety assurance argument could be made. The ontologies provide a definition of the terms used and the relationships between them. The claim structures suggest a possible top-level claim related to the avoidance of harm to people and shows how the claim could be supported. The concept of risk is not used at this stage. This only becomes necessary when product development standards are used, e.g. ISO 26262 [2], ISO 21448 [11].

In March 2025, MISRA SC published the white paper *Uncovering the Historical Road Safety Argument* [7], also referred to as White Paper 2. This white paper explored the historical implicit argument for road safety, the roles of the parties involved and the differences between manually driven and ADS-equipped vehicles. The paper does not address measures to mitigate the severity of an accident after it has occurred; these will be common to both manually driven and automated vehicles.

This paper develops the ideas from white papers 1 & 2, concerning product entity lifecycle phases, harm to people during a lifecycle phase, the role of the vehicle control authority, those implicit historical aims related to the vehicle and its control authority and the parties involved. The result is a model for harm, and the corresponding mitigation measures, in each phase. The safety issues in each phase, and those with associated responsibilities, are discussed and example generic claims are given along with generic topics and their evidence which could be used to support the generic claims. This generic model can then be used to further explore possible missing measures to mitigate harm. The discussion highlights some of the ways in which the move from a human vehicle control authority to an ADS affects the responsibilities.

[1] 'Ontology' — a set of concepts and categories in a subject area or domain that shows their properties and the relations between them

Details of the MISRA SC white papers can be obtained from the MISRA website: https://misra.org.uk/misra-safety-argument/

2 Introduction

2.1 Previous white papers

This white paper draws on a number of ideas developed within white papers 1 and 2.

White Paper 1 [6], includes a product entity ontology which models the relationships between the different product entity lifecycle phases (development, manufacturing, in-service and decommissioning) and the types of people who could be harmed in each of them. It also contains a claim structure for the product entity based on the four lifecycle phases.

White Paper 2, [7], contained models of personal transport on the public roads, the parties involved in the provision of personal transport on the public road network and vehicle movement and harm causation. It also considered the implicit historical argument for road safety, necessary to avoid harm while the vehicle is in-service. The suggestion is to summarise this implicit argument into the seven aims captured in Table 1. White Paper 2 also considers the ways in which the parties helped contribute to meeting the seven aims. The parties referenced in this document include[2]:

- OB4.2.2: *Vehicle Manufacturer*
- OB4.2.3: *Supply Chain*
- OB4.3: *Vehicle Occupants*
- OB4.3.1: *Human Driver*
- OB4.4: *Vulnerable Road Users*
- OB4.6: *Companies operating and managing support services*
- OB12: *Road user*

Aim No	Description
1	That the *road infrastructure* (OB9) to be used by vehicles is suitable and fit for purpose
2	That the *vehicle* (OB10) placed into the public domain is not inherently prone to causing accidents
3	That the *vehicle* (OB10) used is adequate to fulfil the journey
4	That the agent with *vehicle control authority* (OB20) is able to drive in a manner likely to avoid accidents
5	That *vulnerable road users* (OB4.4) have the knowledge, attitude and ability to use the *road infrastructure* (OB9), in a manner likely to avoid accidents
6	That the *vehicle* (OB10) used is the subject of routine maintenance, undertaken by qualified maintenance staff in the protected environment of *companies operating and managing support services* (OB4.6)
7	That the *vehicle* (OB10) is correctly stored and transported by *companies operating and managing support services* (OB4.6), and while not operational on the *road infrastructure* (OB9), is under the responsibility of either the owner or fleet operator

Table 1: Aims to avoid harm for in-service vehicles

[2] The (OBxx) references are taken from the models in White Paper 2.

In this white paper the product entity ontology is developed further to:

- Refine the description of the people intended to have contact with the *product entity*
- Include the features and facilities included in the *product entity* that are used in other lifecycle phases
- Refine the *In-service phase*

The *product entity* claim structure is also developed further, based on the latest ontology. Where relevant, this includes referencing the 7 aims in the discussion about the claims made.

2.2 Product Entity Ontology

An Enhanced Product entity ontology (first introduced in White Paper 1) is shown in Figure 1, the blocks coloured blue indicate those present in the White Paper 1 diagram.

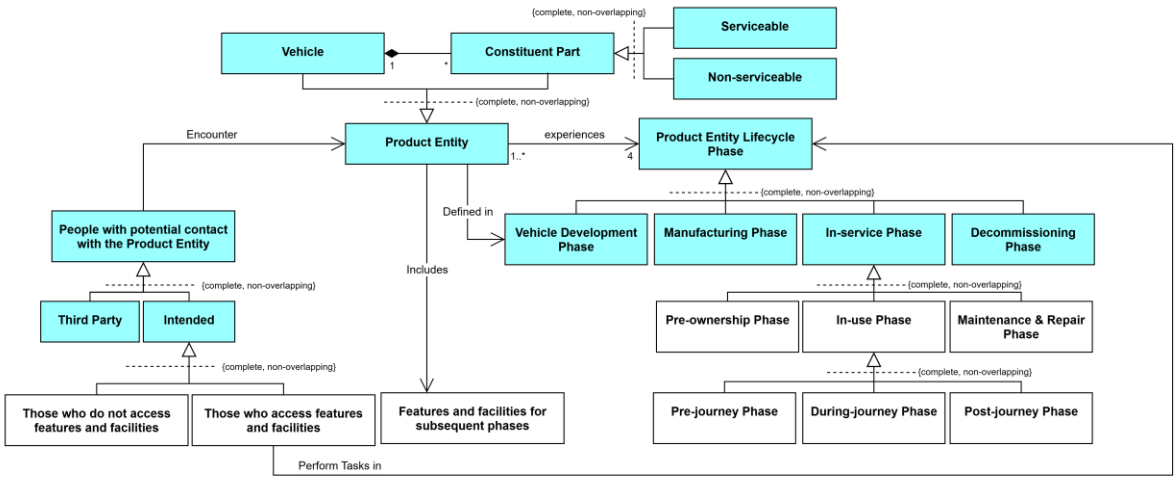


Figure 1: Enhanced Product entity ontology

The ontology includes the term *people with potential contact with the product entity*. This distinction between those people *intended* to come into contact with the product entity and *third parties* applies to all phases except the *in-use phase*. As the *in-use phase* takes place in a public space, distinguishing between individuals' intended and unintended contact with the *product entity* is meaningless. Instead, the term *road user*, OB12, (*vehicle occupants*, OB4.3 and *vulnerable road user*, OB4.4) is used.

People with potential contact with the product entity are also people who could potentially be harmed by the *product entity*. *Third parties* include visitors to industrial and commercial sites as well as those using the public roads. *Intended* people include those who develop, transport, service and use the vehicle. Some of these will make use of, or benefit from, the features & facilities included in the *product entity*.

The *product entity*, which refers to both the *vehicle* and its *constituent parts*, is produced in the *vehicle development phase*. The enhanced product entity ontology acknowledges that there are features & facilities included in the *product entity* explicitly to enable tasks to be performed in the other product entity lifecycle phases.

The enhanced product entity ontology also refines the *in-service phase* into several subphases.

The *pre-ownership sub-phase* covers the time after the vehicle has left the factory but before the owner/user has received it. Activities in this phase include the transport of the vehicle on a vehicle carrier, and the vehicle pre delivery inspection (PDI) at a dealer.

The *pre-journey sub-phase* includes checks to establish that the *vehicle* itself is fit to undertake the journey. The UK government recommend that the correct functioning of lights and brakes should be checked before every journey and that other checks, as stated in the vehicle's handbook be made, e.g. fluid levels (oil, radiator, windscreen washer), battery and tyres. The *pre-journey sub-phase* also includes planning a viable route. There are several reasons why a possible route might not be viable. These include adverse weather conditions such as heavy snow, flooding, extreme cold, extreme winds; geological issues such as landslides, sink holes; and societal issues such as roads restricted by the authorities, riots.

Throughout the *during-journey sub-phase*, features and facilities are used to control the *vehicle*, as the *vehicle* uses the public road to travel from the journey start to the destination. A human driver is expected to adapt to all events and situations throughout this sub-phase, whereas an autonomous vehicle may need to contact other organisations to manage certain situations.

The *post-journey sub-phase* acknowledges that journeys may terminate in several different ways. The most frequent is that of a successful arrival at the desired destination, or an intentional stop during the journey. There is little or no inherent potential for harm given this outcome. However, it may be necessary to stop before the intended destination. Perhaps due to the road network no longer supporting driving (e.g. heavy snow fall), or the *vehicle* developing an issue which means it is no longer able to continue. The human driver is simply expected to manage the situation. However, for a fully autonomous vehicle, it may be necessary for the vehicle to contact other organisations to manage the situation. Additionally, it may be necessary to stop before the destination due to the *vehicle* being involved in a collision or other road incident. At the point of collision, typical *vehicle* actions include activation of secondary safety features such airbags, the unlocking of all doors and calling the response services. Typical post collision actions to make the *vehicle* safe for the emergency services can include disabling all airbags that have not been deployed and cutting off electrical power.

The role of the *maintenance & repair sub-phase* includes the regular maintenance, as required by the vehicle manufacturer, and also repairs as a result of wear and tear and accident damage.

2.3 Vehicle Lifecycle Claims

Within section 2.1, and section 2.2, a number of concepts related to the *vehicle* have been introduced:

- That a vehicle product entity (*vehicle*) has many lifecycle phases
- That harm to people may occur in all of the vehicle lifecycle phases
- That the *vehicle control authority* is responsible for the vehicle behaviour during journeys
- That the implicit historical rationale for preventing harm during a journey included the achievement of a number of aims: Aim 2, Aim 3, Aim 4 and Aim 5.

As described in white paper 1 [6], harm can occur to people working on or around the vehicle. Multiple harm mechanisms exist and could manifest while developing, transporting, servicing or decommissioning the vehicle.

This paper now considers how those who are present, and/or have responsibilities, in each vehicle lifecycle phase contribute to the prevention of harm and how they can claim that they have fulfilled their obligations.

To prevent harm to people in a vehicle lifecycle phase it is first necessary to identify the potential *harm mechanisms* and the circumstances under which the potential may be realised. With this understanding *mitigation measures* can be defined to address the *harm mechanism* and/or mitigate the harm. These *mitigation measures* may be technological and/or people based. Finally, the *mitigation measures* have to be implemented.

Within a phase there are *people with potential contact with the product entity* who may be harmed as a consequence. There are also those in each phase who are responsible for preventing such harm, these people may be those with potential contact with the product entity or they may be removed from it. Either way, they have an obligation to prevent harm and can make a claim regarding their fulfilment of this obligation. This may include claims regarding the communication of information to those with responsibilities in other lifecycle phases. It is noted that a major source of harm in the *during-journey phase* is related to the *vehicle behaviour*, OB14, as determined by the *vehicle control authority,* OB20. These ideas are shown in the ontology in Figure 2. Figure 2 also adds the new entity of *behavioural competences*. These include observable driving behaviours and decision-making capabilities that the *vehicle* demonstrates when interacting with its environment, other road users, and traffic rules. The behaviour exhibited by the vehicle is a reflection of the *behavioural competences* possessed by the *vehicle control authority* (OB20).

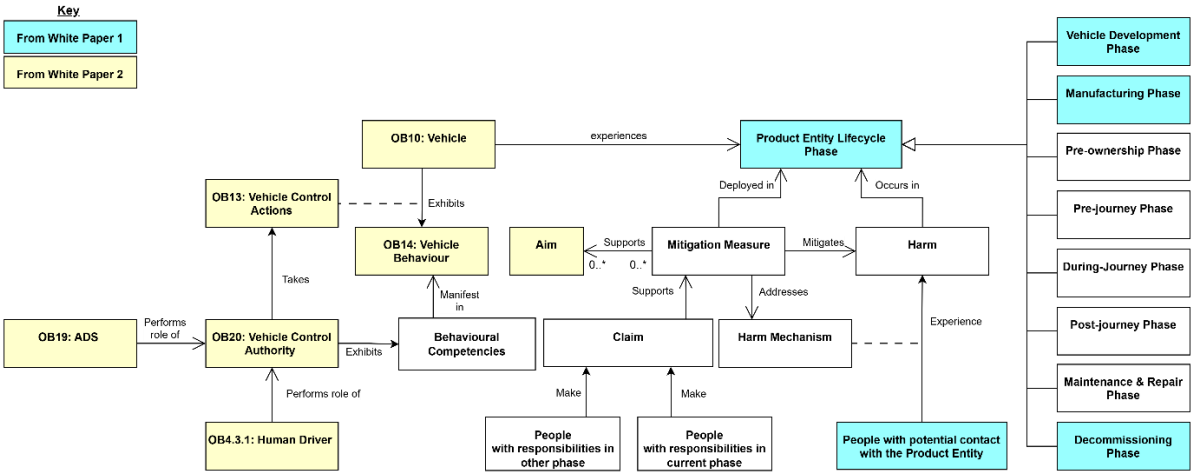


Figure 2: Harm and Mitigation

Several activities related to preventing harm may occur in any phase:

- The potential for harm in the current phase, or another phase, may be identified
- *Mitigation measures* for harm in the current phase, or another phase, may be defined (this may be done in collaboration with the development phase staff)
- *Mitigation measures* requiring implementation in another phase may be communicated to the appropriate body
- *Mitigation measures* for harm in the current phase, or another phase, may be implemented
- Processes may be defined for these activities.

Mitigation measures range from those included in the design of the *product entity*, to process related measures. The *development phase* is unique because many of the *mitigation measures* to prevent harm in later phases have to be included in the design of the *product entity*. They may be identified by the design staff while considering the potential for the behaviour of the *product entity* to cause harm in the later phases, e.g. while performing a hazard and risk assessment. They may be communicated to the design team as a result of analyses performed by staff working in other phases, e.g. requirements coming out of a manufacturing process FMEA.

Those responsible for these activities could make claims regarding the effectiveness of what they have done to identify and mitigate harms. A discussion about these claims is complicated by the fact that the identification of harm and the implementation of its associated *mitigation measures* are not necessarily confined to one phase but may involve multiple phases as illustrated in Table 2. The table also shows which aim is being supported by these activities.

Party	Vehicle Phase	Aim	This Phase Harms	Other Phase Harms	This Phase Mitigations	Other Phase Mitigations
OB4.2.2: Vehicle Manufacturer & OB4.2.3: Supply Chain	Development	2	Identify	Identify	Implement	Implement
	Manufacturing		Identify	Identify	Implement	
OB4.3.1: Human Driver	Pre-journey	3	Identify	Identify	Implement	Implement
	During-journey	3	Identify		Implement	
OB4.6: Companies operating and managing support services	Pre-ownership	7	Identify	Identify	Implement	
	Maintenance & Repair	6	Identify	Identify	Implement	Implement
	Decommissioning		Identify		Implement	
	Post-journey		Identify		Implement	

Table 2: Phases in which harms are identified and mitigation measures implemented

This document discusses *harm mechanisms* generated in each phase. It is important to note that the harm itself can manifest in any phase, not just where the *harm mechanism* originates. Corresponding *mitigation measures* can be allocated within the originating phase or to other phases. To aid reasoning, we assume that prior phases have identified all *harm mechanisms* relevant to those prior phases – or, to put it another way, the *product entity* is not arriving into the current phase with inherent *harm mechanisms*. For example, installing an incorrect software calibration file during the *manufacturing phase* can cause harm during the *in-use phase*. In this example the *harm mechanism* and *mitigation measure* are discussed in the *manufacturing phase* only. This allows the analysis of the subsequent *in-use phase* to assume the *product entity* entering the *in-use phase* is free from inherent causes of harm. In doing so, the *in-use phase* analysis can focus on the activities or functions performed during the *in-use phase* alone, to look for *in-use harm mechanisms*.

Taking this approach has the advantage that when analysing a particular phase, we can ignore any harm originating in other phases, making it easier to think about, but it does have the disadvantage that the phase under consideration may need to make claims about *harm mitigation* implemented in other phases. In doing so, this approach does place a unique burden on the *development phase*, where most of the *product entity's harm mitigations* typically reside.

The claim given for the vehicle in White Paper 1 [6] is:

All appropriate measures have been taken to prevent the vehicle causing harm to people during any of its lifecycle phases when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environment.

With the contexts of:

- *Appropriate Measures*
- *Vehicle*
- *Intended Usage*
- *Reasonably Foreseeable Misuse*
- *Intended Parties*
- *Intended Environments*

As described in White Paper 1, the phrase *appropriate measures* is used as an umbrella term that includes fulfilling safety relevant legal regulations, industry standards/guidelines and local procedures. The measures may also relate to the provision of training or equipment or to the design of facilities.

White Paper 1 also showed a claim structure for the *vehicle* based on the *product entity* lifecycle phases of *development, manufacturing, in-service* and *decommissioning*, resulting in the following sub-claims:

- Vehicle Development Claim
- Vehicle Manufacturing Claim
- Vehicle In-service Claim
- Vehicle Decommissioning Claim

With the refinement of the *in-service phase*, there are now 8 lifecycle phases for which claims can be made, see Figure 1. As there is a common pattern for a claim in each phase, the claim structure from White Paper 1 has been replaced by the one shown in Figure 3.

In the following sections, we discuss the potential for harm in each of the 8 lifecycle phases. This includes suggesting a claim for the measures or mitigations taken in that phase. Typically, this claim would be made by the bodies responsible for the given phase. As part of the discussion, examples are given to highlight the possible *mitigation measures* and evidence produced. Where relevant, the discussion also references one of the 7 aims in Table 1.

In the ontologies discussed thus far, the *product entity* is the subject of each lifecycle phase. However, to simplify the *harm mitigation* discussion (see section 4) we refer only to the *vehicle*. Consequently, from section 4 onwards the *vehicle* becomes the lifecycle phase subject, but often the assertions made will apply equally to the *vehicle* and its *constituent parts*.

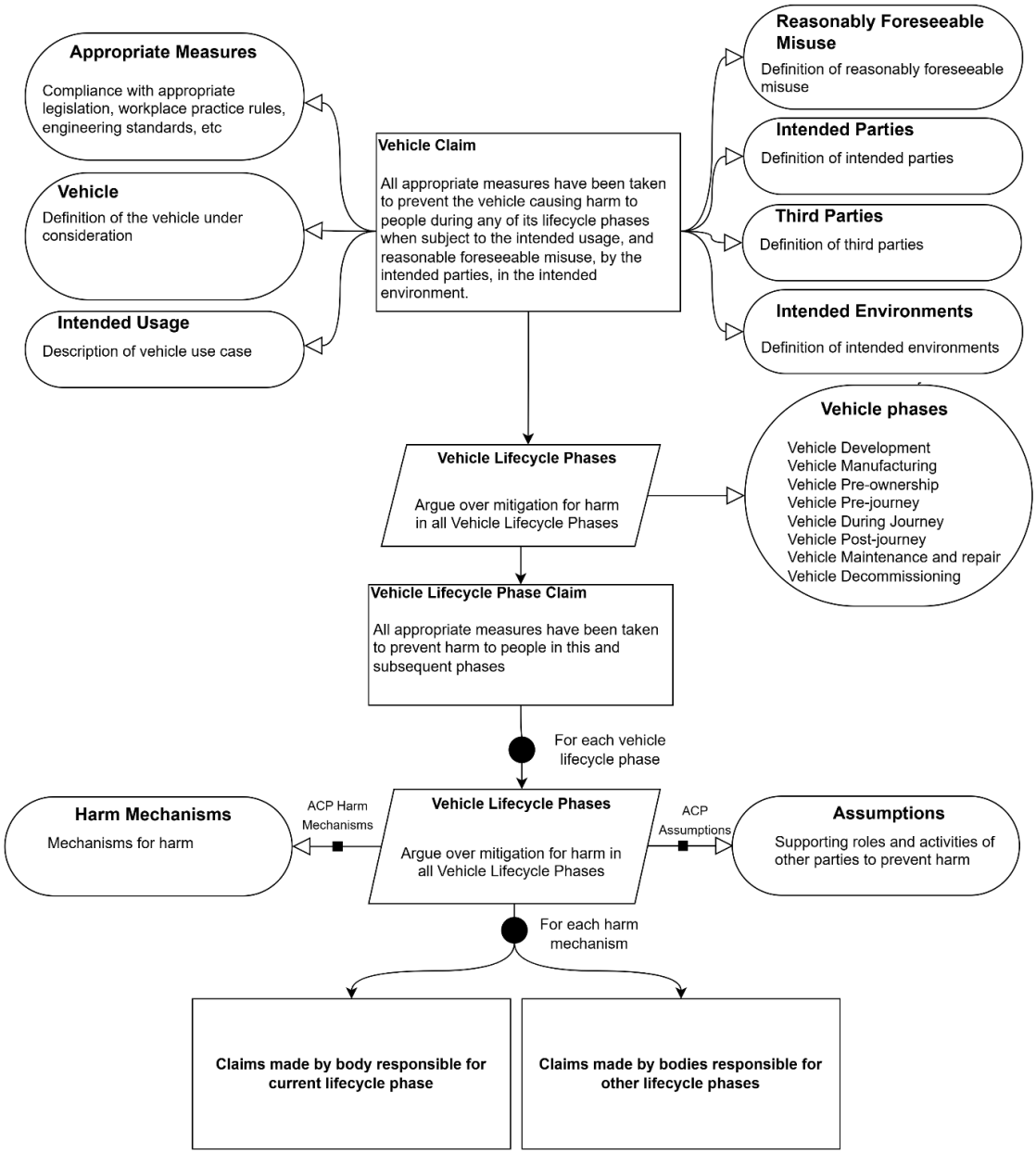


Figure 3: Phase argument pattern

3 Vehicle context

3.1 Vehicle architecture

The *vehicle* can be considered as a base vehicle, with a set of E/E control systems, and a *vehicle control authority* (OB4.3) which uses these systems to control the *vehicle behaviour* (OB14). The *vehicle control authority* may be a *human driver* (OB4.3.1) or an *ADS* (OB19). The base vehicle is controlled by E/E control systems, which are developed in the *development phase*. To distinguish the various vehicle architectural artefacts we use the following terminology within this white paper:

- *Base vehicle*: a complete vehicle comprising the E/E control systems necessary for the vehicle control authority agent to correctly and safely control the vehicle's behaviour.
- *ADS-equipped vehicle*: a complete vehicle, comprising the base vehicle, and an ADS delivering the vehicle control authority responsibility.

- *Vehicle control authority:* the agent responsible for safe and correct vehicle control. The agent can be human or a computer system.
- *Automated Driving System (ADS):* computer system capable of perceiving the environment around the vehicle and commanding the vehicle's actuators as necessary to achieve safe *vehicle behaviour*.

3.2 Vehicle control authority

As introduced above, the *vehicle control authority* (OB4.3) is the agent responsible for achieving safe vehicle control. When the control authority is a *human driver*, they are a key component in the overall vehicle system when it is being driven on the roads. As such, in most countries, this "human component" has to "develop" a minimum maturity and competency before being licensed to become a part of the overall vehicle system. Furthermore, the expectation is that to retain that licence, the "human component" will maintain a satisfactory level of performance.

The development of the "human component" often takes the form of assimilating and understanding the rules of the road (OB6: *Governing Prescriptions*), undergoing a period of supervised learning and passing a short test to establish that they can exhibit good behaviour when controlling the vehicle on the roads and interacting with other road users. Only then is a licence to drive granted. The *human driver* is expected to keep up to date with changes to the rules of the road, possible road layout and road infrastructure changes, and changes to the technology fitted to the vehicle. Road traffic law (e.g. The UK Road Traffic Act) is the legal instrument used by *governments* (OB.4.1) to encourage continued good driving performance.

There is obviously a parallel here with the development of an *ADS* (OB.19), which must also embody the rules of the road, exhibit good behaviour when controlling the *vehicle* and be kept up to date with all changes. The protocols for licensing an *ADS*, as a *vehicle control authority*, and the legal prescription for bad behaviour are immature when compared to that of the *human driver*.

Competency achievement is typically demonstrated within a predetermined envelope (typically referred to as an Operational Design Domain). If the envelope in which acceptable competency was demonstrated changes, then the assumptions under which that determination was made is also subject to change.

3.3 Vehicle Safety

In a *vehicle* safety context, the potential for harm is associated with the behaviour of the completed *vehicle,* e.g. unwanted vehicle movements during manufacturing, transportation, operation and decommissioning. Such *harm mechanisms* are discussed in the latter sections of this white paper. The potential for harm is also associated with the intrinsic properties of the *vehicle* and its components, e.g. high voltages.

The hazard and risk assessment for the E/E systems that comprise the *vehicle* and its *constituent parts* includes identifying the potential for harm in all the *vehicle* lifecycle phases. The output from the hazard and risk assessment will typically identify both the causes of harm, resulting from the operation of E/E systems, and the *harm mitigations* to be implemented by the E/E system.

The *during-journey phase* has historically received the greatest focus, when addressing E/E systems risk, during the *vehicle's* development. With E/E systems development being the subject of standards such as ISO 26262, to manage the risk due to malfunctions of the control system due to random and systematic failures, and ISO 21448 to manage issues related to the insufficiencies in technological solution. To date, ISO 26262 assumes the presence of a *human driver* when assessing risk and the effectiveness of risk *mitigation measures*.

4 Mitigation of harm in lifecycle phases

4.1 Development

4.1.1 Safety Issues

White paper 1 [6], identified 2 categories of people who may come into contact with the *product entity* during the *development phase*: *intended* and *third parties*.

Intended people are those who come into contact with the physical *constituent parts*, and the *vehicle* itself, via virtue of their job. These will typically be the development staff and other authorized personnel, such as the company's managers. Typically, these people encounter the product entity in workshops, labs and test facilities when it may not be fully assembled and when the measures to prevent harm not yet been included or activated. The potential for harm may be inherent in the activity. People classed as *third parties* include visitors to the development facilities. These may also come into contact with the physical *constituent parts* and the *vehicle* itself. When donor or prototype vehicles are used on publicly accessible roads, then the general public may also come into contact with the *vehicle* and may be harmed by an incorrectly functioning vehicle.

4.1.2 Development phase mitigation

The *development phase* is usually subject to health and safety regulations. Typical measures that follow from this, or are common in the industry, include:

- Definition of operating procedures
- Provision of training.
- Use of physical protection
- Quarantining of vehicles
- Restricted access to *vehicle* and *vehicle* systems
- Emergency stop buttons to de-energise the *vehicle* (None of these measures are released into the production *vehicle*)

A comprehensive *development phase* claim that could be made by the *vehicle manufacturer*, OB4.2.2, or company in the *supply chain,* OB4.2.3, is:

Dev_1: All appropriate measures have been taken to ensure all development staff and third parties are not harmed by the vehicle's behaviour in the different environments during development

This claim does not support any of the Aims as these are restricted to the post development phases of the *vehicle* lifecycle.

4.1.3 E/E System Support for Other Phases

A comprehensive claim for the development of the E/E systems is:

Dev_Oth_1: All appropriate measures have been taken to prevent the vehicle causing harm to people encountered during its other lifecycle phases as a result of vehicle behaviour caused by the action, or inaction, of E/E systems.

The results of the *development phase* include measures included in the production *vehicle* intended to prevent harm in other lifecycle phases; discussion of these measures is covered in the phase where the harm may occur and is indicated by the claims prefixed with xxx_Oth.

This claim supports Aim 2 *That the vehicle (OB10) placed into the public domain is not inherently prone to causing accidents.* Where the *control authority* is an *ADS*, then it also supports Aim 4 *That the agent with vehicle control authority (OB20) is able to drive in a manner likely to avoid accidents*.

4.2 Manufacturing

4.2.1 Safety Issues

White paper 1, [6], identified 2 categories of people who may come into contact with the *product entity* during the manufacturing phase: *intended* and *third parties*.

In a manufacturing context, those *intended* to come into contact with the physical *constituent parts* and the *vehicle* itself include the manufacturing staff and other authorised personnel, such as the company's managers. Typically, these people encounter the *product entity* when it may not be fully assembled. The potential for harm may be inherent in the activity. Examples of issues include the use of high voltage in electric *vehicles* and unintended actuation of torque sources whilst the *vehicle* is being assembled.

People classed as *third parties* include visitors to the manufacturing plant. These may also come into contact with a partially assembled *vehicle*.

Incorrectly assembled *product entities* can cause harm in subsequent lifecycle phases. Examples include:

- Inappropriate calibration data is allowed to be installed into a *vehicle* during the *manufacturing phase* that can cause unintended *vehicle behaviour* during the *in-service phase*
- Incorrect connection of an airbag to the electrical firing circuit in the *manufacturing phase* may render the feature non-functional during the *in-service phase* or affect the safe disposal of the airbag

4.2.2 Manufacturing phase mitigation

A comprehensive *manufacturing phase* claim that could be made by the *vehicle manufacturer*, OB4.2.2, or company in the *supply chain* OB4.2.3 is:

Man_1: All appropriate measures have been taken to prevent the vehicle causing harm to manufacturing staff and plant visitors and, by its behaviour, to people encountered during subsequent lifecycle phases.

The manufacturing phase is usually subject to health and safety regulations. Typical measures that follow from this, that are common in the industry, include:

- Definition of operating procedures
- Provision of training
- Use of physical protection
- Quarantining of *vehicles* and *constituent parts*
- Restricted access to *vehicle* and vehicle systems

This claim supports Aim 2 *That the vehicle (OB10) placed into the public domain is not inherently prone to causing accidents.*

The operating procedures will include facilities included in the product during development as discussed in the next section.

4.2.3 Development phase mitigation

A comprehensive *development phase* claim in support of the *manufacturing phase* that could be made by the *vehicle manufacturer*, OB4.2.2, or company in the *supply chain* OB4.2.3, is:

Man_Oth_1: All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to enable the manufacturing plant to construct the vehicle without it causing harm to the staff and plant visitors and, by its behaviour, to people encountered during its other lifecycle phases

Examples of design measures include:

- *Vehicle* configuration self-checks to prevent non-approved calibration data being installed
- Benign default configured *vehicle* state for manufacturing that requires appropriate authorisation to transition out of during *vehicle* commissioning
- Facilities to prevent actuation of torque sources, particularly important for *ADS vehicles* since the *vehicle control authority* is physically part of the *vehicle*.
- High voltage interlock (HVIL) combined with plausibility checks before the HV system can be activated
- On board vehicle diagnostics to report non-connected airbags.

4.3 Pre-ownership

4.3.1 Safety issues

The *pre-ownership phase* is a sub-phase of the *in-service phase*, see Figure 1. This sub-phase encompasses all *in-service* activities that take place, following the completion of the *manufacturing phase,* but before the *vehicle* goes into use. Key aspects include transportation, pre-delivery inspection (PDI) through a dealer network and *vehicle* handover to the owner or operator. *Intended* and *third parties* have the potential to come into contact with the *product entity* during the *pre-ownership phase*.

People *intended* in the *pre-ownership phase* will typically be the *vehicle* transportation staff moving *vehicles* from the place of manufacture to the dealerships and dealership staff performing the PDI. For these people, an encounter with the *product entity* is an encounter with a fully assembled and fully functional *vehicle*. Within this sub-phase, the potential for harm relates to unintended vehicle movement, either whilst the *vehicle* is being transported or inspected. An example of potential harm for transportation staff could relate to a *vehicle* fitted with deployable side-steps that are intended for easy of ingress and egress. If the side-steps were to deploy in a confined space, with a person present, that person could be crushed or trapped. Similarly, for anyone performing PDI activities, any unexpected *vehicle* actuator movement can cause harm, from automatic windscreen wipers to unexpected steering or torque actuation.

People classed as *third parties* include the general public in the vicinity of transported *vehicles* and visitors to the dealership. They can also be affected by unintended movement of the *vehicle* or its constituent parts.

In addition to harm caused directly within this phase, harm can be indirectly caused in the subsequent *in-service phase*. Examples could include unexpected *vehicle behaviour* due to incorrectly prepared *vehicles* during the PDI, such as failing to remove covers from sensors and disabling any transport only features of the *vehicle*. Also, incorrect use of *vehicle* features (including automated driving features) could cause unexpected *vehicle behaviour*, due to the failure to exchange all relevant information

during the *vehicle* handover. Limitations of automated features should be of specific interest here, such as when the *human driver* needs to resume control of an automated function, etc.

4.3.2 Pre-ownership phase mitigation

A comprehensive *pre-ownership phase* claim that could be made by the *vehicle manufacturer* (OB4.2.2), or *transport and dealership companies* (OB4.6) is:

Pre-o_1: All appropriate measures have been taken to prevent the vehicle causing harm to people during its pre-ownership phase and, by its behaviour, to people encountered during the In-use phase

The *pre-ownership phase* is usually subject to health and safety regulations. Typical measures that address harm in the *pre-ownership* and *in-use* phases, or are common in the industry, include:

- Provision of training
- Definition of operating procedures
- Activating and deactivating a transport mode
- PDI checklists
- Handover checklists
- Adherence to health and safety at work procedures

The claim above supports Aim 7, *That the vehicle (OB10) is correctly stored and transported by companies operating and managing support services (OB4.6), and while not operational on the road infrastructure (OB9), is under the responsibility of either the owner or fleet operator.*

The operating procedures will use functions included in the product during development as discussed in the next section.

4.3.3 Development phase mitigation

A comprehensive *development phase* claim in support of the *pre-ownership phase* that could be made by *engineering developers and manufacturers* (OB4.2) is:

Pre-o_Oth_1: All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to enable pre-ownership activities without them causing harm to the staff and, by its behaviour, to people encountered during its other lifecycle phases

Design measures could include a specific transportation mode to prevent unwanted *vehicle* movements during transportation. For automated vehicles the *vehicle control authority* is physically part of the *vehicle* and has full access to the *vehicle* actuators. In this case specific transportation modes would need to restrict the ability of the *vehicle control authority* to make unwanted actuator requests.

4.4 Pre-journey

4.4.1 Safety issues

Once the *vehicle* is operational (i.e., it is being used by the final customer), checks are typically undertaken *pre-journey* – that is, prior to the *vehicle* beginning its journey. The purpose of these *pre-journey* checks is twofold. Firstly, to ensure that the *vehicle* is ready and able to undertake that journey

safely[3] , and secondly to ensure that passengers are positioned correctly before the journey commences.

White paper 1, [6], identified 2 categories of people who may come into contact with the *product entity* during the *pre-journey phase*: *intended* and *third parties*. During the *pre-journey phase* itself, the *intended* category comprises the person undertaking the *pre-journey* checks and the *vehicle occupants* – both of whom are at risk of harm during the *pre-journey phase*. No *third parties* relevant to the *pre-journey phase* are identified.

There are four themes of harm identified in relation to *pre-journey* checks, namely:

- Harm caused performing a pre-journey phase check: for example, harm could be caused by crushing or entrapment if the *vehicle* and *vehicle* systems have not been properly secured before the *pre-journey* checks begin. In addition, if the remedial action requires topping up fluids (e.g., windscreen washer fluid) then the person performing the checks may need to adhere to the safe handling requirements specified on the chemical's safety data sheet to avoid harm. However, such safe handling requirements are outside of the scope of this discussion. It is important to note that *pre-journey* checks include both inspection and redress. For all types of *vehicle control authority* (OB20) a human will be involved in the redress aspects, even if the inspection relies on built in features.
- Harm caused by not performing a pre-journey phase check: for example, the loss of *vehicle* control, due to a rapid tyre deflation, could result in harm occurring during the *journey phase*. However, with the rapid tyre deflation potentially due to the *vehicle* being operated with incorrect tyre pressures, the cause of harm is the failure to check and adjust the *vehicle's* tyre pressures in the *pre-journey phase*.
- Harm caused by incorrectly positioned passengers: typically, just prior to commencing a journey, checks are made in and around the passenger compartment to avoid harm occurring during the journey. This might involve ensuring that all doors are closed and secure, and checking that passengers are correctly seated with their seat belts fastened. If such things are not checked prior to the journey commencing, then there is the potential for harm to result during the *journey phase* itself.
- Harm caused by incorrect route planning: another potential cause of harm could result from errors in journey route planning. For example, routing the *vehicle* into an area that is either unsafe or unsuitable for the *vehicle* could result in the *vehicle* occupants being put in harm's way during the journey. The same could be said for planning a journey with insufficient range to complete the journey and the *vehicle* left stranded on the highway with the occupants at risk. It should be noted that route planning is an activity that is ongoing throughout the journey.

4.4.2 Pre-journey phase mitigations

An overarching claim that can be made by the *vehicle manufacturer* (OB4.2.2) in relation to the *pre-journey phase* is given below.

Pre-j_1: All appropriate measures have been taken to prevent the vehicle causing harm to people during its pre-journey phase and, by its behaviour, to people encountered during the Journey phase

This claim supports Aim 3, That the *vehicle* (OB10) used is adequate to fulfil the journey.

[3] The UK Highway Code recommends that the correct operation of lights and brakes is checked before every journey, together with any additional checks suggested by the *vehicle manufacturer* in the vehicle's handbook. The vehicle's handbook might direct the *human driver* to check fluid levels (e.g., oil, radiator, windscreen washer), battery state and tyre pressures.

The introduction of automation increases the dependency on the *development phase* mitigation, where some of the responsibility to implement checks is moved from the *human driver* (OB4.3.1) to the ADS-equipped vehicle. Mitigation is discussed below for the four main themes of harm identified.

HARM CAUSED PERFORMING PRE-JOURNEY CHECKS

Pre-journey checks are usually subject to health and safety regulations, however, the extent to which health and safety regulation applies will be dependent on the environment that the checks are performed in and by whom.

Typical measures that follow from this, or are common in the industry, include:

- Definition of operating procedures (*vehicle* owner's manual for private ownership, or further procedures for fleet owned *vehicles*)
- Provision of training (for fleet owned *vehicles*)
- Activating and deactivating a maintenance mode (for human based checks and remedial activities)
- Adherence to health and safety at work procedures (for fleet owned *vehicles*).

Pre-journey safety issues relate to any harm that could be caused to persons undertaking the prescribed *pre-journey* checks and remedial activities. This might require the *vehicle* to be placed in a safe and secure state before the checks commence. In a manual driving context, ensuring that the *vehicle* is safe and secure would typically be the responsibility of the *human driver*.

HARM CAUSED DUE TO NOT PERFORMING THE PRE-JOURNEY CHECKS

In a manual driving context, mitigating harm caused due to not performing *pre-journey* checks would be provided by operating procedures and guidance supplied in the *vehicle* manual by the *vehicle manufacturer* (OB4.2.2) as well as requirements from *government and agencies* (OB4.1) to perform certain checks. The ability of a *human driver* to know how to perform certain checks is part of the driving test in the UK. The examiner will ask two questions from a longer list that confirms that the driver knows how to check the condition of tyres, critical fluid levels, functions of steering and braking etc. before starting a journey. This forms part of the pass and fail criteria in the UK.

In an automated driving context, the role may still be with the *human driver*, or it may fall to some other organisation or individual (e.g., *companies operating and managing support services* OB4.6). For example, ensuring that all necessary Robotaxi *pre-journey* checks have been carried out, might fall to a Fleet Operator employee. In this case, mitigation would be provided in the same form as in the manual driving context and through operating procedures. However, the role of performing certain checks may be transferred to the ADS-equipped vehicle and require *development phase* mitigations.

HARM CAUSED DUE TO INCORRECTLY POSITIONED PASSENGERS

In the UK, all *vehicle occupants* (OB4.3) over the age of 14 are responsible for their own seatbelts. Below that age the *human driver* (OB4.3.1) is responsible. This also includes the deactivation of passenger airbags when using rear facing child seats and correct seating and seatbelt positioning for children. Therefore, for a *human driver* (OB4.3), mitigation is provided by the *vehicle manufacturer* (OB4.3.1) through the definition of operating procedures (*vehicle* owner's manual) and by *government and agencies* (OB4.1) through legal requirements. There is an assumption that the *human driver* has the competencies and knowledge necessary to correctly fit child seats and to deactivate passenger air bags as required.

For ADS-equipped vehicles such as a Robotaxi, the role to ensure that passengers are correctly positioned before starting a journey may also be fulfilled by a human. For fleet owned vehicles the human may be remote from the vehicle. This would require mitigation of additional operating procedures defined by the fleet operator detailing safe positioning of passengers before allowing the journey to commence. Alternatively, the fleet operator may place the responsibility on the passenger who made the original booking, through service terms and conditions. In this case the fleet

operator would need to provide operational procedures of sufficient detail to ensure the responsible passenger is able to undertake the mitigating actions effectively. For private ownership it is unclear how this role would be fulfilled as passengers under the age of 14 could travel alone. Potentially this role could be shared between the *vehicle* owner and the ADS-equipped vehicle. Journeys could be authorised by the *vehicle* owner in a similar way to fleet ownership, either in person or remotely using video confirmation and *vehicle* status data. It is also possible that the ADS-equipped *vehicle* may fulfil this role entirely, in which case all mitigation is handled in the *development phase*.

HARM CAUSED DUE TO INCORRECT ROUTE PLANNING

For a manually driven *vehicle*, correct route planning depends on the competence of the *human driver* (OB4.3.1) and the information presented by the *vehicle* (e.g. calculated route from the navigation system, *vehicle* range, fuel and energy levels). Other than the supporting *development phase* requirement for accurate *vehicle* information, the *pre-journey phase* mitigation relies upon the common sense of the *human driver* (OB4.3.1). It would be generally expected that a human planning a route would check the suitability of the roads, weather, *vehicle* range and any other factors that are required for a successful journey. These are human skills learnt through other types of activities and applied to driving. No specific mitigation measures are required. Even with the use of satellite navigation apps and devices, it is expected that the *human driver* is responsible for checking the suitability of the proposed route, along with the other associated factors.

For automated driving the route planning factors could be checked by a human, either the *vehicle* owner or someone working for a fleet operator remote from the *vehicle*, or the confirmation of a suitable route could be performed completely by the ADS. For the fleet owned case, mitigation measures would include operational procedures to ensure consistent journeys. Where the ADS takes the journey confirmation role, all mitigation is handled within the *development phase*. In both cases, the checking and planning could be based around pre-defined approved routes or acceptability criteria as well as available live traffic information.

4.4.3 Development phase mitigations

Vehicle manufacturer (OB4.3.1) claim:

A claim by the *vehicle manufacturer* or (company in the *supply chain* (OB4.2.3)) regarding design actions taken to support the ADS-equipped vehicle's safe operation during the *pre-journey phase* is:

Pre-j_Oth_1: All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to enable the pre-journey activities to be carried out without them causing harm to the staff and, by its behaviour, to people encountered during its other lifecycle phases.

HARM CAUSED PERFORMING PRE-JOURNEY CHECKS

Vehicle design measures needed might include the ability to prevent *vehicle* movement during remedial activities (e.g. powertrain longitudinal movement, air suspension vertical body movement, or roll control *vehicle* body roll). Additional restrictions around automated vehicles would need to be taken into consideration – for example, restricting their ability to request *vehicle* actuations. These measures may be fully automated, including detection and reaction within the vehicle design, or they may require intervention by a human. Examples of these could be a special service mode requiring human interaction that prevents vehicle powertrain actuations, or a feature that prevents park brake disengagement whilst the vehicle bonnet is unlatched.

HARM CAUSED DUE TO NOT PERFORMING THE PRE-JOURNEY CHECKS

For the manual driving context, no Development Phase mitigation is required, but the addition of automation into the *vehicle* may need its own dedicated checks. Potentially, an ADS-equipped *vehicle* will perform its own *pre-journey* checks to replace the *human driver* responsibility. This might

involve inhibiting the *vehicle* if the *vehicle* itself deems that is not in a fit state to undertake the journey. For example, an ADS-equipped *vehicle* may measure the tyre pressures to be below the minimum required and prevent the *vehicle* from exceeding a defined safe speed threshold until it is corrected. Although the checks themselves could be performed by the *vehicle*, any remedial action (such as topping up fluids and tyre pressures) will typically to be performed by a human, again putting that human operator potentially in harm's way. Mitigation for this is discussed elsewhere.

HARM CAUSED DUE TO INCORRECTLY POSITIONED PASSENGERS

Development phase mitigation is required for both the manually driven context and for ADS-equipped *vehicles*. This includes:

- Availability of live *vehicle* data, such as:
  - Door status
  - Seatbelt latch status
  - Seat occupied status
  - Airbag deactivation status

This data allows a human or an ADS-equipped *vehicle* to determine if there are problems with the positioning of passengers.

For ADS-equipped *vehicles*, any remote confirmation that a journey is safe to start would require the real-time transmission of *vehicle* data, including live video footage of the passengers, and the ability to prevent a journey starting. For levels of automation that require no human intervention, the ADS-equipped *vehicle* would need be able to determine the type and location of each passenger and evaluate if it is safe to start the journey. This competence would need to be included in the design along with the proof of its integrity.

HARM CAUSED DUE TO INCORRECT ROUTE PLANNING

For both manual and automated driving, development phase support requires the provision of correct *vehicle* data by the *vehicle manufacturer* (OB4.2.2). This includes any fault states, *vehicle* range etc. In the case where the ADS takes the entire role of safe route planning, the ADS needs to be designed with a demonstrable competence to derive a safe and correct route. In addition, the ADS will require data provided by *companies operating and managing supporting services* (OB4.6). This includes weather reports, incident reports, road status data, map data etc. This data would need to be of high quality and in real-time. The *development phase* would need to include the provision for receiving this live data and also potentially broadcasting data gathered during a journey.

4.5 During journey

4.5.1 Safety Issues

Perhaps the most obvious mechanism for harm occurring during the journey itself, is in an accident. This could be the result of *vehicle behaviour* (OB14) not commanded by the *vehicle control authority*, inappropriate *vehicle behaviour* due to a lack of competency, or failure of the *vehicle* to respond to control actions by the *vehicle control authority*. Examples of insufficient competence could include, not following the rules of the road or social etiquette (i.e. *governing prescriptions* (OB6)), an unawareness of the current *vehicle* capability, an unawareness of changing road and weather conditions, and the lack of anticipation of other road users. During an accident candidates for harm include any *road users* (OB12) (e.g. vehicle occupants, and vulnerable road users). During the journey phase there are no *third-party* candidates for harm.

Lack of competency can be due to inadequacies either in the *vehicle control authority's* (OB20) ability to control the *vehicle* in the current conditions or an inadequacy in the services provided by the

supporting parties, e.g. the road infrastructure is not fit for purpose (see Aim 1). There are many parties and roles, detailed in White Paper 2, that provide or support accident *mitigation measures* (see aims 1 through 5). These aims form the main assumptions for the *during-journey phase*, and in doing so places the focus on the *vehicle control authority* (OB20) for the mitigation.

In addition to the harm caused by an accident, we also need to consider the potential harm generated by having incorrectly positioned passengers in the *during-journey* phase. This was first identified in the *pre-journey* phase, so this considers the situation where at the start of the journey all passengers were positioned correctly, but afterwards this changes. For example, a passenger unclips their seatbelt after the vehicle begins the journey.

4.5.2 Journey phase mitigations

In both a manual and automated driving context, the *vehicle control authority* (OB20) has responsibility for the following claim:

Dur-j_1: All appropriate measures have been taken to prevent the vehicle causing harm while in the during-journey phase.

Harm caused due to inadequate behavioural competencies

The central mitigation is that there is an unimpaired and suitably trained *vehicle control authority* (OB20) making requests of the *vehicle* (OB10). In a manual driving context, achieving the correct *vehicle behaviours* would be down to the human driver's actions. In an automated driving context, it would be the *ADS vehicle control authority's* predefined *behavioural competencies* and actions that dictate the resultant *vehicle behaviour*. For both types of *vehicle control authority* (OB20) continuous feedback is required to obtain an appropriate control response. This can include feedback on *vehicle* (OB10) system malfunctions, weather conditions, etc.

In the manual driving case, the minimum level of competency is demonstrated by obtaining a driving licence through standardised examination, controlled through *government and agencies* (OB4.1). It is also important to note, that this is a minimum level and there is an expectation that the *human driver* will grow their competency level over time, through experience gained. It is never anticipated that the entire transport service is populated solely with newly qualified *human drivers*. Therefore, the larger proportion of other *human drivers* with greater experience are expected to accommodate and anticipate the *behavioural competency* weaknesses of newly qualified drivers. In the case of an *ADS*, the minimum level of *behavioural competency* is determined at the development phase. Functionality needed to achieve the required mitigation, through *vehicle behaviour*, is discussed in section 4.5.3. It could be expected that the level of *behavioural competence* demonstrated by an *ADS vehicle control authority* needs to exceed that of a newly qualified *human driver*, and there are several reasons for this. The first is that updates in behaviour for the *ADS* are not real-time and there will be a delay in validating and releasing new software. The second is that there are more new cars registered each year than there are newly qualified drivers each year (four times more based on UK statistics from 2024). This could dilute the average level of *behavioural competence* in the transport system if all new *vehicles* are fitted with *ADS* capabilities that are not equivalent to that of an experienced *human driver*. Society in general will not tolerate 'mistakes' by AD-equipped *vehicles*, therefore the competency expected will likely need to be better than a 'careful and competent' *human driver*.

Harm caused due to incorrectly positioned passengers

As with the *pre-journey* phase, in the UK, all *vehicle occupants* (OB4.3) over the age of 14 are responsible for their own seatbelts. Below that age the *human driver* (OB4.3.1) is responsible. Therefore, for a *human driver* (OB4.3), mitigation is provided by the *vehicle manufacturer* (OB4.3.1) through the definition of operating procedures (*vehicle* owner's manual) and by *government and agencies* (OB4.1) through legal requirements. There is an assumption that the *human driver* has the competencies and knowledge

necessary to ensure that passengers under their responsibility are positioned correctly throughout the journey.

For ADS-equipped vehicles such as a Robotaxi, the role to ensure that passengers are correctly positioned throughout the journey may also be fulfilled by a human. For fleet owned vehicles the human may be remote from the vehicle. This would require mitigation of additional operating procedures defined by the fleet operator detailing safe positioning of passengers throughout the journey. Alternatively, the fleet operator may place the responsibility on the passenger who made the original booking, through service terms and conditions. In this case the fleet operator would need to provide operational procedures of sufficient detail to ensure the responsible passenger is able to undertake the mitigating actions effectively. For private ownership it is unclear how this role would be fulfilled as passengers under the age of 14 could travel alone. Potentially this role could be shared between the *vehicle* owner and the ADS-equipped vehicle. The ADS-equipped *vehicle* could monitor the status of doors, seatbelt latches and airbag deactivation mechanisms resulting in the termination of the journey and requiring refreshed authorisation from the owner to continue. This would require further mitigation from the *vehicle manufacturer* (OB4.2.2) through operating procedures (*vehicle* owner's manual) and supporting design considerations. It is also possible that the ADS-equipped *vehicle* may fulfil this role entirely, in which case all mitigation is handled in the *development phase*.

4.5.3 Development phase mitigations

A comprehensive development phase claim in support of the *during-journey* phase that could be made by *engineering developers and manufacturers* (OB4.2) is:

Dur-j_Oth_1: All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to ensure no harm is caused by the vehicle during the vehicle journey

Achieving the above claim supports a *vehicle control authority* (OB20) of any type, as well as developing the *ADS behavioural competency*.

HARM CAUSED DUE TO INADEQUATE BEHAVIOURAL COMPETENCIES

Design mitigations in support of the *vehicle control authority* include indicating the current capability of the *vehicle* as, irrespective of the type of *vehicle control authority*, key control decisions, and hence vehicle safety, rest on the knowledge of the *vehicle* state.

Vehicle capability information could include:

- Error states
- Interventions by vehicle systems (stability control, etc.)
- Levels of available traction
- Vehicle range
- Present speed
- Selected gear
- Etc.

The achieved *ADS behavioural competency* is critical and is challenging to prove, but is a core design mitigation. Evidence from the Typical Evidence table in Annex B can be used to support a *behavioural competency* argument.

It includes:

- Controlling the *vehicle* within its current capability
- Operating within the constraints of the law
- Accounting for environmental conditions

- Reflecting behaviours that are courteous and consistent with the social norms for that region
- Exhibiting a defensive driving style.

The notion of *behavioural competencies* and the use of *behavioural competencies* to describe the appropriateness and sufficiency of the *vehicle control authority's* (OB20) actions is the subject of a future MISRA White Paper.

HARM CAUSED DUE TO INCORRECTLY POSITIONED PASSENGERS

Development phase mitigation is required for both the manually driven context and for ADS-equipped *vehicles*. This includes:

- Availability of live *vehicle* data, such as:
  - Door status
  - Seatbelt latch status
  - Seat occupied status
  - Airbag deactivation status

This data allows a human or an ADS-equipped *vehicle* to determine if there are problems with the positioning of passengers.

For ADS-equipped *vehicles*, any remote confirmation that a journey is safe to continue would require the real-time transmission of *vehicle* data, including live video footage of the passengers, and the ability to terminate a journey safely. For levels of automation that require no human intervention, the ADS-equipped *vehicle* would need be able to determine the type and location of each passenger and evaluate if it is safe to continue the journey. This competence would need to be included in the design along with the proof of its integrity.

4.6 Post-journey

4.6.1 Safety issues

In the *post-journey phase*, those *intended* to come into contact with the *vehicle* are the *vehicle occupants*, other *road users* and emergency services personnel. During the *post-journey phase* there are no *third-party* candidates for harm.

As noted in section 2.2, a *vehicle* journey may terminate in several different ways including:

- The successful arrival at the desired destination, or an intentional stop during the journey
- The premature termination of the journey due to adverse weather conditions or a *vehicle* issue
- The premature termination of the journey due to collision.

Despite having successfully arrived at the desired destination, without the *vehicle* inflicting harm, the potential still exists for harm to be caused when passengers exit the vehicle. For example, cyclists passing by the *vehicle* could be harmed by a vehicle door opening into their path. The *vehicle occupants* themselves may incur harm because they cannot see the surface onto which they are stepping or they misjudge the distance to the ground – this is particularly relevant for *vehicle* with active suspension systems.

A journey may end prematurely due to adverse weather conditions, *vehicle* failures or lack of fuel or battery power. In such cases harm may result. For example, if *vehicle occupants* are unable to contact support services or if those support services have difficultly determining the precise location of the *vehicle*.

Unfortunately, a journey may be ended prematurely due to a collision with other road users, the road infrastructure or natural objects. During the collision the *vehicle occupants* may incur harm, typically blunt trauma injuries caused either by *vehicle* body deformation, or by their movement during the collision by not being adequately restrained.

After a collision, the *vehicle occupants* may be unable to egress the *vehicle*, or they may be exposed to the harmful effects of fire or high voltages. Emergency service personnel attending the *vehicle* incident may also be exposed to the effects of fire or high voltage. Emergency service personnel may also be harmed by unexpected movement of the *vehicle* or *vehicle* body. The inability to physically move the *vehicle* may hamper efforts to manage a situation. The detonation of still primed and active pyrotechnic devices is also a potential source of harm. It is also necessary to stop in these circumstances and not continue the journey until all parties involved are content.

If a journey ends prematurely, due to a collision, understanding why the collision occurred is an important step in reducing the likelihood of harm for road users in general. Examples of past investigations into *vehicle* collisions include claims by the *human driver* of unintended acceleration or unintended braking. For an ADS-equipped *vehicle*, the resultant *vehicle behaviour* and the *vehicle control authority's* dynamic driving task (ref. SAE J3016) actions that lead to that behaviour, may need to be understood. This requires storage and retrieval of data concerning the *vehicle* dynamic state as well as the internal parameters of the *ADS* related to sensing, understanding, deciding and acting. The results of an investigation into the causes of a collision may be of relevance to several bodies, including *engineering developers and manufacturers* (OB4.2) and *government and agencies* (OB4.1).

4.6.2 Post-journey phase mitigation

In both a manual and automated driving context, the *vehicle control authority* (OB20) has responsibility for the following claim:

Post-j_1: All appropriate measures have been taken to prevent the vehicle causing harm while in the post-journey phase.

Upon arrival at the desired destination, or when making an intentional stop during the journey, the *vehicle control authority* (OB20) is responsible for ensuring that the *vehicle* comes to rest in a suitable place. Likewise, the *vehicle occupants* are responsible for taking care while egressing the vehicle. Furthermore, for driverless taxi services, additional functionality may be needed to help passengers with reduced mobility exit the vehicle safely. For example, lowering the vehicle ride height. The *vehicle control authority* may also have some responsibility for determining when it is safe for the passengers to egress the *vehicle*. For example, this could mean keeping the doors of an ADS-equipped vehicle locked if there are people in its vicinity who could be hit by a door as it is opened.

If the *vehicle control authority* (OB20) terminates the journey prematurely, perhaps because of a significant *vehicle* fault, it is responsible for ensuring that the *vehicle* stops in a suitable place, and for obtaining any necessary assistance. The *vehicle control authority* is also responsible for ensuring that other road users are aware of the presence of the stationary *vehicle* in the road. Ensuring that other road users are afforded sufficient time to respond, is typically achieved using the *vehicle's* hazard lights and by the placement of a warning triangle several metres behind the *vehicle*.

If the journey terminates prematurely, as a result of a collision, then what happens next will likely be influenced by the damage done to the *vehicle* and its occupants. In a manual driving context, if damage to the *vehicle* is slight then the human driver could be expected to move the *vehicle* to a safe place, make others aware of the presence of the stationary vehicle (e.g. by way of warning triangle placement, etc.), and obtain the necessary roadside assistance. For an *ADS-equipped vehicle*, the *vehicle control authority* (OB20) may be capable of moving the *vehicle* to safety, but more typically will require

intervention by a remote human operator to achieve this task. The remote operator or other support personnel may also be responsible for guiding the *vehicle occupants* regarding making the *vehicle* conspicuous to others. If the damage to the *vehicle* or occupants is severe, then the actions available to the *vehicle control authority* (be that human or *ADS*) may be limited. In such situations, it may be left to the *vehicle's* eCall (emergency call) function to register the collision and to notify the emergency services of the *vehicle's* location. Appropriate measures will also need to be considered for the safe handling, transportation and storage of a crash damaged *vehicle*. In addition to the physical hazards posed by the base vehicle technology, the ADS-equipped vehicle will require processes involving the emergency and recovery services to disable or manipulate the *vehicle control actions* (OB13). For a Robotaxi this is likely to involve interactions with the vehicle's teleoperations team.

4.6.3 Development phase mitigation

A comprehensive *development phase* claim in support of the *post-journey phase* that could be made by the *vehicle manufacturer* (OB4.2.2), or company in the *supply chain* (OB4.2.3), is:

Post-j_Oth_1: All necessary information has been communicated to those responsible for the development phase to allow appropriate design measures to be included in the design to prevent harm to the vehicle occupants and third parties in the post-journey phase and, by its behaviour, to people encountered during its other lifecycle phases

Design measures to facilitate the safe egress of *vehicle* occupants may include the provision of puddle lights and child locks. In addition, functions to detect and warn occupants of nearby objects or the approach of other road users may be deployed. To notify others of the stationary vehicle's presence, requires the provision of marker lights, hazard lights and warning triangles.

Design measures deployed to support the *vehicle occupants*, should the journey end prematurely include the addition of an eCall function that can contact the support services and, with wide geographical coverage, determine and report the *vehicle's* location. For ADS-equipped vehicles, it may be the responsibility of the *ADS* (as *Vehicle Control Authority*) to find a suitable location to stop the *vehicle*. In addition, design measures may be deployed that enable a human operator to control and safely move the ADS-equipped *vehicle* (assuming suitable safety rigour can be demonstrated).

Design measures that help prevent harm in the event of a collision include post collision braking, the provision of seat belts, seat belt pretensioners and airbags. To help minimise the harm to *vulnerable road users*, the vehicle bonnet may be released to lessen a bonnet impact, or external airbags may be deployed. The vehicle body is designed to both deform on impact, both to absorb impact forces and to reduce the extent to which it intrudes into the occupants' cabin space.

Examples of design measures that help prevent further harm after a collision include automatic release of the door locks, the severing of power supplies and isolation of high voltage sources. In addition, the *vehicle manufacturer* will typically create and publish procedures, for emergency first responders, to assist in handling a post-collision *vehicle*.

Possible design measures to support collision investigation activities include facilities to record the *vehicle* dynamic state and, where appropriate, the internal parameters of the *ADS*, such that that data is preserved during the collision.

4.7 Maintenance & Repair

4.7.1 Safety issues

The *maintenance & repair phase* is part of the *in-use phase* and includes activities such as routine servicing, the replacement of worn parts and the repair to damage caused by collisions. The environment and candidates for harm are different, but like the *manufacturing phase*, during the *maintenance and repair phase* the *vehicle* could be disassembled by varying degrees. In addition, like the *manufacturing phase*, both *intended* and *third-party* individuals may come into contact with the *vehicle* during this phase.

Maintenance and repair phase activities potentially take place in several locations. In a workshop environment (e.g. service or tyre centres), those *intended* to encounter the *vehicle* are workshop staff. In a less formal setting, the *intended* people could be roadside assistance staff or *vehicle* owners undertaking home repairs. These people encounter the *vehicle* in various conditions. These states include fully operational, undefined fault states and physical damage through collisions. The potential for harm within this phase is concerned with unintended *vehicle* movement or exposure to other sources of harm such as high voltage or thermal events. An example could be replacing or repairing high voltage system components in a partially assembled *vehicle*.

People classed as *third parties* include the general public in the vicinity of a non-workshop repair and visitors to a repair workshop such as vehicle owners, insurance assessors etc.

In addition to harm caused directly within this phase, harm can be indirectly caused in the subsequent *in-use phase*. Examples could include unexpected vehicle behaviour due to incorrectly repaired or calibrated *vehicles*, such as the incorrect calibration of ADAS vision and radar systems. Harm could also be caused in the *decommissioning phase* by incomplete / poor repairs or by the fitment of substandard components.

4.7.2 Maintenance & Repair phase mitigation

A comprehensive *maintenance & repair phase* claim that could be made by *companies operating and managing support services* (OB4.6) is:

> *M&R_1: All appropriate measures have been taken to prevent the vehicle causing harm while in the Maintenance & Repair phase and, by its behaviour, to people encountered during the In-use phase.*

The claim above supports Aim 3, *That the vehicle (OB10) used is adequate to fulfil the journey*.

When the *maintenance & repair phase* activities are performed in an official workshop environment, they are usually subject to health and safety regulations. Typical measures that follow from this, or are common in the industry, include:

- Provision of training.
- Adherence to health and safety at work procedures
- Use of Physical Protection Equipment (PPE)
- Definition of operating procedures
- Restricted access to the *vehicle*
- Correct use of *vehicle* features

The required operating procedures will use facilities included in the product during development as discussed in the next section. For the high voltage example, a combination of the above measures could be appropriate to control direct exposure of people to high voltage.

Where maintenance & repair activities take place in an unofficial, unregulated environment, a plausible assurance claim becomes much more difficult to make. Any activities undertaken by those not appropriately trained, or in possession of the appropriate equipment, do so at their own risk and are not covered by any claims made by an official organisation. Given that we acknowledge that these environments exist and operational procedures and training may be weak, then stronger *development phase* mitigation may be required to support these use cases with their known deficiencies.

4.7.3 Development phase mitigation

A comprehensive Development phase claim in support of the *maintenance & repair phase* that could be made by *engineering developers and manufacturers* (OB4.2) is:

M&R_Oth_1: All necessary information has been communicated to those responsible for the development phase activities to allow appropriate design measures to be included in the design to prevent the vehicle causing harm to people during its maintenance & repair phase and, by its behaviour, to people encountered during the In-use and decommissioning phases

Vehicle design measures needed might include the ability to prevent *vehicle* movement during servicing (e.g., powertrain longitudinal movement, air suspension vertical body movement, or roll control *vehicle* body roll), disabling a safety feature (e.g., air bags), or calibrating *vehicle* control systems having replaced a worn or broken part (e.g., replacing an air suspension height sensor, or a tyre pressure monitoring pressure sensor). Additional restrictions would need to be considered for automated *vehicles*. This could include, restricting the *ADS* (*Vehicle Control Authority* (OB20)) from commanding *vehicle* actuators while service actions are undertaken.

Given that operational procedures and training may be weak in certain maintenance & repair environments, automatic disabling through tamper recognition and recommissioning through special service tools may be required. For example, any detected break in continuity of the high voltage interlock loop (HVIL) whilst the *vehicle* is stationary automatically shuts down the HV battery and opens the main HV contactors. Recommissioning of the HV and closing of the main contactors is only possible after the *vehicle* has successfully performed its own continuity check of the HVIL.

4.8 Decommissioning

4.8.1 Safety issues

The *decommissioning phase* has many similarities with the *manufacturing,* and *maintenance & repair phases*, in that both *intended*- and *third-parties* typically come into contact with a partially assembled *vehicle*.

Intended people will typically be the decommissioning staff, handling the *vehicle* in different states of dismantlement and damage – from a fully functioning *vehicle*, to a malfunctioning or crash damaged *vehicle*, through to a *vehicle's* component parts. An example *harm mechanism* could be exposure to high voltage due to a crash damaged *vehicle*. As with the *maintenance & repair phase*, the environment that a *vehicle* is decommissioned in may not be easily controlled and more dependency will be placed on the *development phase* mitigation.

People classed as *third parties* include visitors to the decommissioning facilities and couriers of the individual disassembled parts.

4.8.2 Decommissioning phase mitigation

A comprehensive *decommissioning phase* claim that could be made by *companies operating and managing support services* (OB4.6) is:

Decom_1: All appropriate measures have been taken to prevent the vehicle causing harm to decommissioning staff and visitors

When the *decommissioning phase* is performed in an official workshop environment, this is usually subject to health and safety regulations. Typical measures that follow from this, or are common in the industry, include:

- Provision of training
- Adherence to health and safety at work procedures
- Use of physical protection
- Definition of operating procedures
- Restricted access to the *vehicle*
- Correct use of *vehicle* features.

For the high voltage example, a combination of the above measures could be appropriate to control direct exposure of people to high voltage.

When decommissioning takes place in an unofficial, unregulated environment, making a credible decommissioning claim is difficult. Any activities undertaken by those not appropriately trained, or in possession of the appropriate equipment, do so at their own risk and are not covered by any claims made by an official organisation. Given that we acknowledge that these environments exist and operational procedures and training may be weak, then stronger *development phase* mitigation may be required to support these deficiencies.

4.8.3 Development phase mitigation

A comprehensive *development phase* claim in support of the *decommissioning phase* that could be made by *engineering developers and manufacturers* (OB4.2) is:

Decom_Oth_1: All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to ensure no harm is caused by the behaviour of either the vehicle or vehicle sub-assemblies during decommissioning

Vehicle design measures needed might include the ability to prevent *vehicle* movement during disassembly (e.g., powertrain longitudinal movement, air suspension vertical body movement, or roll control *vehicle* body roll) or prevent exposure to other sorts of hazards like high voltage. Additional restrictions around automated *vehicles* would need to be taken into consideration, restricting their capability of requesting *vehicle* actuations.

Given that operational procedures and training may be weak in certain decommissioning environments, automatic disabling of automated *vehicle* requests, actuators and HV through tamper recognition may be required. See the HVIL example from the previous section. A service disconnect feature to manually disable HV on the *vehicle* is also a critical design measure, but relies on operatives following operational procedures to be effective. Therefore, this alone would be weak mitigation for the hazards identified in this phase.

5 During Journey GSN Argument

In this section we look at the *during journey phase* assumptions, claims and evidence that one can present for an ADS-equipped vehicle having high- or full-automation. By way of an example, we have taken the safety argument pattern from Figure 3 and instantiated it for an ADS-equipped *vehicle*. See Figure 4. As discussed previously, the claims made are from a *vehicle* design perspective.

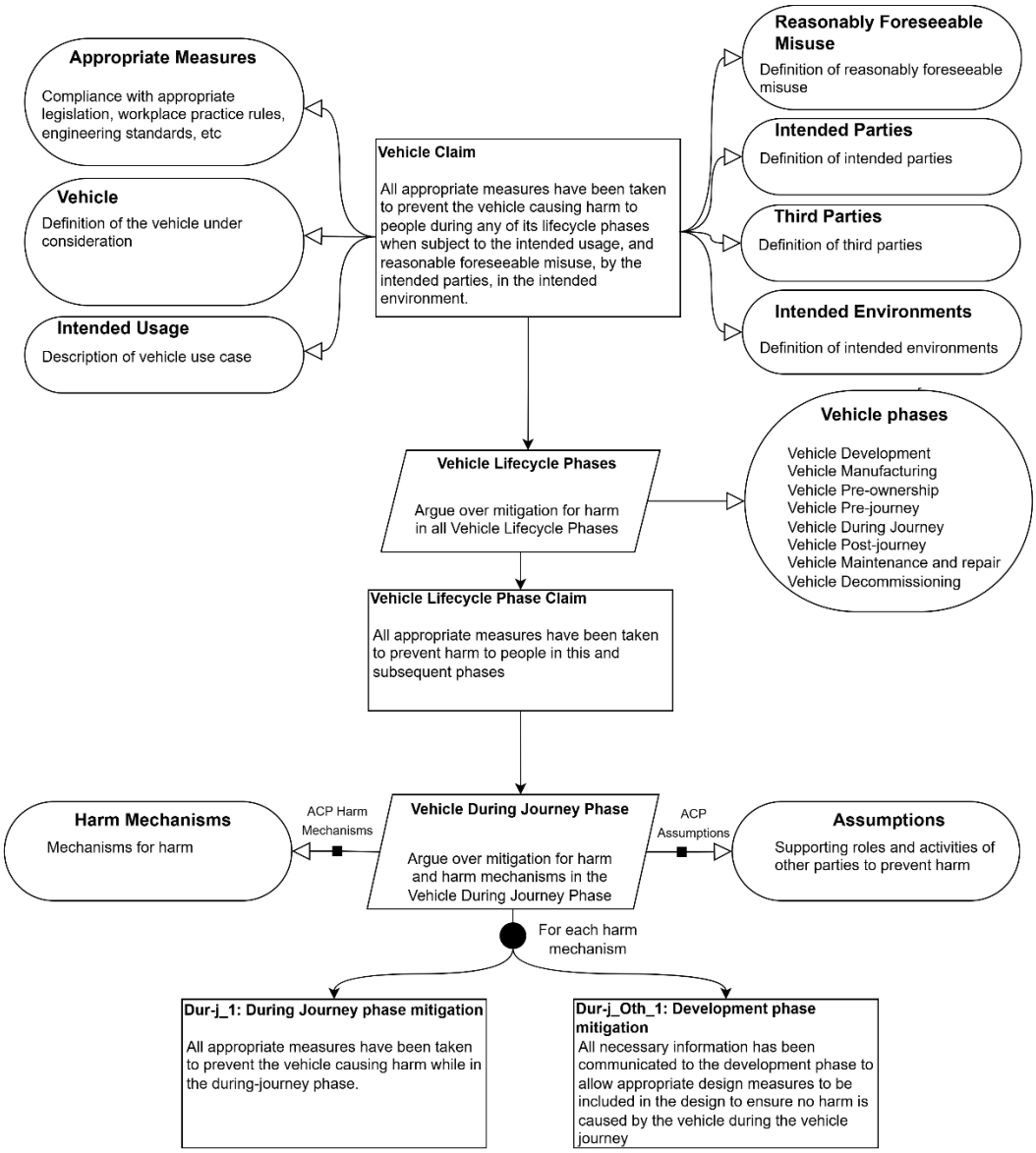


Figure 4: Example journey claim structure for an ADS-equipped *vehicle*

5.1 Overall context

Table 3 gives examples of contextual information that one might use to populate the upper context elements in Figure 4. Note, because they appear at the top of the diagram, these contextual assertions apply to all *vehicle* lifecycle and all *vehicle* journey phases.

Context	Description
Appropriate Measures	E.g. compliance with ISO 26262, ISO 21448, UK Automated Vehicles Act 2024 (AVA 2024) etc
Vehicle	Fully autonomous taxi. Max 6 passengers. No steering wheel or conventional driver controls. Unladen weight 2,500 kg. Limited to 70mph (intended). Ingress / egress on both sides of the *vehicle*. Adult and child restraints, including ISO child seat interface. 5G communication to remote back-office broadcasting *vehicle* data, including interior and exterior video.
Intended Usage	Autonomous ride hailing. Maximum 6 secured passengers. Payload 1,000kg. City taxi service operating on mapped and defined roads. Remote human back-office support making non time-critical decisions.
Reasonably Foreseeable Misuse	>6 passengers. 1 or more unsecured passengers. Payload exceeding 1,000kg. Etc.
Intended Parties	*During journey* specific *intended* parties: - *Vehicle Passengers* (OB4.3.2) - *Road Users* (OB12) including *Vulnerable Road Users* (OB4.4)
Third Parties	For the *during journey* phase, there are only *intended* parties. No *third parties.*
Intended Environments	Uniform and segmented road surfaces only. For use on mapped and defined roads. Not suitable for use in snow or significantly reduced visibility.
Vehicle Phases	As specified in the figure.

Table 3: Generic context

5.2 ADS during journey context

This section concerns the context and claims made for the *during journey phase* (lower half of Figure 4). The ontology in Figure 2 describes how *harm mechanisms* contribute to causing *harm* to people, and how appropriate *mitigation measures* are devised to mitigate those *harm mechanisms*. For the argument about the avoidance of harm to be convincing, all *harm mechanisms* must be identified and mitigated. The list of *harm mechanisms* must be justified and evidenced, and must remain valid for the duration of the ADS-equipped *vehicle's* deployment. An Assurance Claim Point (ACP) is included (see Figure 4) to justify the complete and correct list of *harm mechanisms* defined.

To explore and better understand the wider implications of an *ADS vehicle control authority* in the harm and mitigation causal chain, we have expanded the ontology (beyond the *human driver* (OB4.3.1) element in Figure 2), to encompass both human and ADS behaviours. See Figure 5. The *human driver* context is included for symmetry, but the focus (and the relationships of interest) is with the *ADS* (OB19) as the *vehicle control authority* (OB20). Figure 2 models the manifestation of *behavioural*

competencies as observable *vehicle behaviour* (OB14). Figure 5 shows that the possession of *behavioural competencies* can only be assessed by observing the *vehicle behaviour* (OB14).

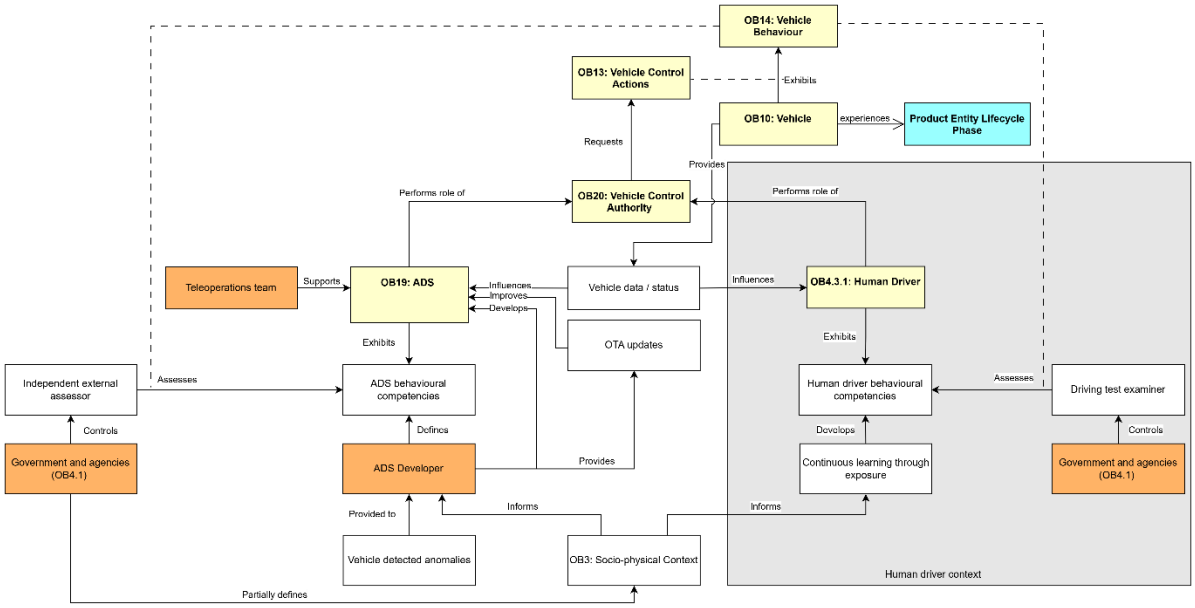


Figure 5: Extended Harm and Mitigation

Using the roles and relationships in Figure 5, *harm mechanisms* can be identified by considering the impact of deficiencies. For example, *intended parties* could experience harm, as a result of undesirable *vehicle behaviour* (OB14) in the *during journey phase*, caused by inappropriate *vehicle control actions* (OB13) by the *vehicle control authority* (OB20). For this example we are focusing on the *ADS*, where *harm mechanisms* can be identified by considering system-level deficiencies. Particular attention is placed on the *ADS* itself (including development interfaces) as well as support deficiencies from the *teleoperations team*. The following sections illustrate examples of *harm mechanisms* and possible *mitigation measures*.

A point to note is that in this example *government and agencies* (OB4.1) has two roles. The first is to partially define the *socio-physical context* (OB3) and the second is to control the assessment of the *ADS behavioural competencies*.

5.3 Teleoperation Team example

5.3.1 Harm identification

Focusing on the *teleoperations team*, they monitor the ADS-equipped *vehicle* fleet remotely and can intervene when the *ADS* requests support – having encountered a complex, ambiguous, or "edge case" scenario that it cannot navigate independently. In addition, the *teleoperations team* can speak directly to *vehicle occupants* via the *vehicle's* audio system to provide reassurance or instructions during a delayed or redirected ride. The *teleoperations team* cannot request 'direct' *vehicle control actions* from the *ADS*, instead they provide high-level commands, such as "proceed," "change lane," or drawing a new, safer path on a map for the *vehicle* to follow. Each operator will be responsible for a fleet of *vehicles*, so will not be continuously monitoring each Robotaxi.

To explore *harm* and *harm mechanisms* relating to teleoperation for a high-automation Robotaxi, we consider the accident scenario of a pedestrian being hit by the Robotaxi. In our specific example, the Robotaxi has collided with a pedestrian and immediately stopped on the carriageway with the pedestrian still under the *vehicle*. Having collided with the pedestrian, the *ADS* requests support from

the *teleoperations team* on how to proceed. A scenario such as this, could be considered a part of the *during journey phase* or, equally, as a part of the *post journey phase*.

The reader could identify further examples from other sources, including a report by the Department for Transport, 'User requirements to enable passengers of automated passenger service (APS) to perform journey tasks during emergencies' [15]. This document considers several emergency scenarios and the interactions between passengers and automated transport.

5.3.2 Harm mechanisms

Reflecting on the role of the *teleoperations team* – to provide the *ADS* with correct high-level information on how to proceed – we can apply failure-mode guidewords to identify potential *harm mechanisms* in the provision of information by the *teleoperations team*:

- No information
- Delayed information
- Information without request
- Incorrect information
- Partial information.

Had this accident scenario happened while the *vehicle* was being driven by a *human driver*, then one could reasonably expect the human driver to:

- Secure the *vehicle*, not allowing any movement unless absolutely necessary
- Apply hazard lights
- Check on the condition of the pedestrian
- Call the emergency services and provide them with a full account of what happened
- Set up a warning triangle (if appropriate).

By considering the action necessary to aid the injured pedestrian and secure the accident scene, with the *teleoperations team* suffering information failures, we identify potential *harm mechanisms* for the Robotaxi's remote operation. The *harm mechanisms* identified appear in Table 4.

It is important to note that this is a partial example and the failings of the *vehicle* to provide appropriate information to the *Teleoperations team* is also important, but not discussed here.

Guidewords	Failure Mode	Effect / Harm
No information	• *ADS* not instructed to move in the presence of additional immediate danger (e.g. fire) • *ADS* not instructed to secure the vehicle	• Pedestrian further injured. • Emergency services not informed. • Occupants harmed
Delayed information	• *ADS* not instructed to move in the presence of additional immediate danger (e.g. fire) • *ADS* not instructed to secure the vehicle	• Pedestrian further injured. • Emergency services delayed. • Occupants harmed
Information without request	• Not applicable	• Not applicable
Incorrect information	• *ADS* instructed to park at the side of the road or to continue with the journey. • *ADS* not instructed to move in the presence of additional immediate danger (e.g. fire) • *ADS* not instructed to secure the vehicle	• Pedestrian further injured. • Emergency services not informed. • Occupants harmed
Partial information	• *ADS* not instructed to secure the *vehicle* • *ADS* not instructed to move in the presence of additional immediate danger (e.g. fire)	• Pedestrian further injured. • Emergency services not informed. • Occupants harmed

Table 4: Failure modes and effects – collision with pedestrian

5.3.3 Dur-j_1During Journey Phase Mitigation

Having identified potential *harm mechanisms*, we now consider the *during journey phase* mitigations deployed to satisfy the following argument claim:

All appropriate measures have been taken to prevent the vehicle causing harm while in the during journey phase.

In order for the *teleoperations team* to provide the required response they would need to be:

- Available within a short time of the request
- Aware that the vehicle has stopped due to a collision
- Aware of video footage of the vehicle surroundings before and after the collision
- Aware of where the pedestrian is now located
- Aware of any other hazards posed by the situation
- Aware of the local emergency procedures in the country the Robotaxi is located.

Harm has been identified if the information from the *teleoperations team* is prevented, delayed, incorrect or incomplete. Therefore, typical appropriate measures to mitigate this harm include;

- *Teleoperations team* structure – limited number of Robotaxi's allowed per teleoperator (headcount ratio) to enable appropriate availability of a teleoperator
  - This must accommodate all time critical scenarios with an appropriate availability
- Operational procedures for teleoperators' situational awareness and localised emergency procedures

5.3.4 Dur-j_Oth_1Development Phase Mitigation

Having identified potential *during journey phase* mitigations, we now consider the *development phase* mitigations deployed to satisfy the following argument claim:

All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to ensure no harm is caused by the vehicle during the vehicle journey

Situational awareness is important in this example, as it affects the teleoperator's decision making ability. Therefore, if the teleoperator is to perform their operational procedures successfully, then consideration of the following design measures is typically needed during the *development phase*:

- High integrity (including availability) data connection between the *vehicle control authority* and the *teleoperations team*
  - Accounting for loss of 5G networks, loss of power supply at the teleoperation centre, loss of power supply at the Robotaxi etc.
- Ability of the *vehicle control authority* to detect and report all types of collisions (not just those that typically require airbag deployment)
- Ability of the *vehicle* to provide the teleoperator with:
  - *Vehicle* location
  - Video footage from around the *vehicle* – both before and after the collision
  - Two way audio communication with *vehicle occupants*
- After a detected collision the *vehicle control authority* must stop the *vehicle*, make itself visible to other traffic, contact the *teleoperations team*, provide the required data and perform as instructed.

5.3.5 Assumptions

There is an assumption that the *pre journey* and *maintenance phases* are fully addressed, i.e. it is a fully maintained and working base *vehicle* that starts the journey. This reduces the scope of the *harm mechanisms* to the phase being assessed.

5.4 ADS example

5.4.1 Harm identification

While operational within the Operational Design Domain (ODD) the *ADS* (OB19) exhibits *ADS behavioural competencies*. These *ADS behavioural competencies* will have been defined, developed and implemented by the *ADS developer*. The *ADS developer* will develop the *ADS behavioural competencies* cognisant of the *socio-physical context* (OB3) the *ADS*-equipped vehicle is being developed for; providing the rules, expectation and environment for which there are numerous inputs and dependant roles supporting the definition. See White Paper 2 [7] Figure 1 for further details.

The *ADS behavioural competencies* are unlikely to remain static over time. The *ADS's* initial behaviour may undergo change, having been assessed by *Government and Agencies* (OB4.1) as part of the commissioning process. Changes in *vehicle status* / data may also require the *ADS* to modify its behaviour during the *during journey phase* – e.g. reduction in performance due to the loss of a redundant sensor or actuator. In addition, field data collected while the ADS-equipped *vehicle* is operational may uncover *vehicle* detected anomalies requiring further *ADS behavioural competency* development. In-service modifications to the *ADS behavioural competencies* will typically take place via *OTA updates*.

For this example, we take the specific *during journey phase* scenario of the *ADS* making an emergency braking request when not required. This leads to *harm* in the form of a rear end collision with a

following *vehicle*. By identifying the entities having relationships to the *ADS behavioural competencies* (see Figure 5), and considering the impact that failures in those relations will have on *ADS behaviour*, we can identify potential *harm mechanisms* requiring mitigation.

5.4.2 Harm mechanisms

When considering the scenario of an emergency braking request when not required, multiple failures can be identified which could be categorised as *harm mechanisms*. To illustrate the ideas, this example selects only a small sample of potential *harm mechanisms*; as uncovering a complete definition of *harm mechanisms* would be a significant task. Table 5 considers how different traffic barrier types (e.g. metal, concrete, wire rope, roadside barriers used to constrain vehicle movement) present within the ODD, may adversely affect *ADS* behaviour leading to an *ADS* emergency braking request when not required.

Entity	Failure Mode	Notes
ADS Developer	• Incomplete / incorrect behaviour defined and developed for all possible types of traffic barriers (shape, size and material), in all weather conditions and in all regions of deployment	• Undesirable behaviour released allowing false detection of other *vehicles* in close proximity
Socio-physical context	• Incomplete definition of all possible types of traffic barriers (shape, size and material) • Incomplete definition of all regions for deployment • Incomplete definition of all types of weather conditions	• Undesirable behaviour released allowing false detection of other *vehicles* in close proximity
OTA updates	• Updates not delivered • Updates not implemented • Updates delayed • Updates corrupt	• Undesirable behaviour released or allowed to persist, allowing false detection of other *vehicles* in close proximity
Vehicle data / status	• Design using a single sensor set (e.g. camera, radar or LiDAR) with physical limitations in traffic barrier detection in all environmental conditions • Redundant sensor set for sensor fusion unavailable • Low quality sensor data for traffic barrier detection • Incorrect interpretation of base vehicle data	• Poor detection capability of the *ADS*, leading to exhibiting poor *behavioural competencies*, allowing false detection of other *vehicles* in close proximity
Government and agencies (OB4.1)	• Incomplete assessment of *behavioural competencies* involving traffic barriers • Incomplete definition of all possible types of traffic barriers (shape, size and material)	• Does not prevent *vehicles* with poor *behavioural competencies* being deployed, allowing false detection of other *vehicles* in close proximity • Prevents the *ADS* behaviour being developed with all possible traffic barriers, allowing false detection of other *vehicles* in close proximity
Vehicle detected anomalies	• Failure to report all instances of emergency braking requests	• Undesirable behaviour allowed to persist, allowing false detection of other *vehicles* in close proximity

Table 5: Failure modes related to an undesirable brake request from the ADS

5.4.3 Dur-j_1During Journey Phase Mitigation

Having identified potential *harm mechanisms*, we now consider the *during journey phase* mitigations deployed to satisfy the following argument claim:

All appropriate measures have been taken to prevent the vehicle causing harm while in the during-journey phase.

All *harm mechanisms* identified relate to the deficiencies in the development of the *ADS*, so are addressed in section 5.4.4.

5.4.4 Dur-j_Oth_1 Development Phase Mitigation

We now consider the *development phase* mitigations deployed to satisfy the following argument claim:

All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to ensure no harm is caused by the vehicle during the vehicle journey

Section 9 lists typical topics and typical evidence that may be used as the basis for appropriate measures in different phases. A selection of typical topics have been referenced in Table 6 which extends the failure modes of interest from Table 5.

Entity	Failure Mode	Typical Topics
ADS Developer	• Incomplete / incorrect behaviour defined and developed for all possible types of traffic barriers (shape, size and material), in all weather conditions and in all regions of deployment	• TE02 - The robustness of the autonomous control authority against the defined infrastructure • TE05 - The consistency of the behaviour of the *vehicle* and *vehicle control authority* • TE12 - The assurance of the correct use of the base *vehicle* controls • TE14 - The measures to address deficiencies previously identified by independent assessment • TE27 - The adequacy of the Safety Policy to provide an appropriate level of safety • TE28 - The implementation of the Safety Policy • TE29 - The maintenance and updating of the Safety Policy • TE30 - The maintenance of consistent *vehicle* capability and suitability for use within the ODD • TE32 - The *vehicle control authority* meets the driving performance criteria for its licensed usage • TE33 - The ability to restrict the operation of the *vehicle* to regions where it is presently licensed • TE34 - The ability of the *vehicle control authority* to meet and maintain a pre defined driving ability • TE35 - The adequacy of the *Safety Policy* to incorporate all relevant ethical, legal and insurance / societal expectations
Socio-physical context	• Incomplete definition of all possible types of traffic barriers (shape, size and material) • Incomplete definition of all regions for deployment • Incomplete definition of all types of weather conditions	• TE01 - The completeness of the knowledge of the infrastructure requirements • TE06 - The completeness of the knowledge of the environment that the *vehicle* is intended to be deployed in
OTA updates	• Updates not delivered • Updates not implemented • Updates delayed • Updates corrupt	• TE15 - The timeliness with which issues arising during operation are mitigated • TE18 - The periodic updating of the vehicle to account for all official changes • TE31 - The timeliness of the updates made to the *vehicle* in response to field performance, road infrastructure changes, legal changes etc.

Entity	Failure Mode	Typical Topics
Vehicle data / status	• Design using a single sensor set (e.g. camera, radar or LiDAR) with physical limitations in traffic barrier detection in all environmental conditions • Redundant sensor set for sensor fusion unavailable • Low quality base vehicle data for traffic barrier detection • Incorrect interpretation of base vehicle data	• TE04 - The robustness of the engineering of the base *vehicle* • TE10 - The adequacy of the base *vehicle* performance, including its limits, for the intended purpose • TE13 - The correctness of the interface between the *vehicle control authority* and the OEM vehicle platform controls • TE16 - The adequacy of the warnings and diagnostic information provided to the *vehicle control authority* • TE24 - The ability to monitor changes in *vehicle* performance throughout the duration of the journey • TE25 - The response of the *vehicle control authority* to changes in *vehicle* performance
Government and agencies (OB4.1)	• Incomplete assessment of all driving scenarios involving traffic barriers • Incomplete definition of all possible types of traffic barriers (shape, size and material)	• Included as part of Assumptions, Section 5.4.5
Vehicle detected anomalies	• Failure to report all instances of emergency braking requests	• TE08 - The assurance of correct field operation

Table 6: Failure Modes and Typical Topics

5.4.5 Assumptions

Again, there is an assumption that the *pre journey* and *maintenance phases* are fully addressed, i.e. it is a fully maintained and working base *vehicle* that starts the journey. This reduces the scope of the *harm mechanisms* to the phase being assessed. It is also assumed that *Government and agencies* (OB4.1) will have performed a complete and correct assessment of the *ADS* behaviour as well as fulfilling their role in the definition of the *socio-physical context* (OB3) by defining all official traffic barriers.

6 Summary of responsibility transfer from human to ADS vehicle control authority

The nature of the claims changes when the *vehicle control authority* is an *ADS* rather than a *human driver*, as the *ADS* cannot perform all the traditional tasks. This particularly affects claims related to *pre-journey, during-journey* and *post-journey*.

The *pre-journey* claims (Pre_j_1 & Pre-j_Oth_1) concern providing the information necessary for the *pre-journey* checks and then ensuring that these can be carried out without causing *harm*. That the checks are carried out, and that any remedial actions necessary are taken, has been the responsibility of the *human driver*.

While an ADS-equipped vehicle may be able to perform most of the checks mentioned in section 4.4.1, there will be some that it cannot e.g. deactivation of passenger airbags when using rear facing child seats. In the cases where only a human can take any necessary remedial action, then the user will need to be clearly informed of this responsibility.

If the ADS-equipped *vehicle* determines that the *vehicle* is not fit to undertake the journey, an option would be for the *vehicle* to disable itself. However, there is often a balance between *harm* that may occur if the journey is undertaken and the *harm* that may occur if the journey is not undertaken. This balance may be judged in favour of undertaking the journey by a human being if they deem it urgent to leave a situation or to reach a destination. There is a need to address such dilemmas, for example having contact with a remote operator, for a fleet *vehicle*, or a phone app for a privately owned *vehicle*.

The *during-journey* claims (Dur-j_1 & Dur-j_Oth_1) are about ensuring that the *behavioural competencies* of the *vehicle control authority* are sufficient to undertake the journeys that the *vehicle* is likely to be required to do, as discussed in section 4.5.2. The threshold for sufficiency is usually based on a comparison with the performance of *human drivers*. The challenge for the design of an *ADS*, which takes the responsibilities of the *vehicle control authority*, is to achieve the appropriate level of *behavioural competency*, as discussed in section 4.5.3.

The *post-journey* claim (Post-j_Oth_1) is about ensuring that *harm* is avoided however the journey ends. In the case of successful arrival at the desired destination, there is little difference between a *vehicle* driven by a human being and an ADS-equipped vehicle, e.g. securing the vehicle. In the case of a journey being terminated prematurely, for an ADS-equipped vehicle, any actions necessary, as mentioned in section 4.6.2, are the responsibility of the *vehicle*, e.g. stopping in a suitable place, unlocking the doors to allow passengers to exit the *vehicle*, or contacting the remote operator for assistance.

In the *pre-ownership, maintenance & repair* and *decommissioning phases* the mitigations that may be used to support the claims are related to avoiding movement of the *vehicle*, or its accessories, as appropriate. The need for these claims only arises in ADS-equipped vehicles.

7 Summary of Work to Date

In this series of white papers we have made the case that motorised transport on the public roads is a service. Many parties are involved in delivering this service and all have a role to play in preventing *harm* to the people using it, or those who are just present on the roads. Each party has their own understanding of what is required of them, and they operate largely independently from the other parties. While there is no one body that is wholly responsible for the entire service, there is a tacit understanding of how the different contributions combine to prevent *harm*. Seven aims have been formulated to capture this understanding. Ideally all parties would document a justification of why they believe what they have done is sufficient. This is starting to happen for *vehicles* with standards requiring safety cases.

Considering the contribution made by those parties responsible for the design of the *vehicle* and its components, the case has been made that the *vehicle* has a lifecycle, and *harm* may occur in any phase. *Harms* in one phase may be identified in a different phase while the mitigations for *harms* in one phase may be implemented in a different phase. All parties have a responsibility to do their best to avoid *harms* in any phase.

These ideas have been set in a more formal context by using ontologies to define the terms used. Ontologies for the following have been produced:

- Service view of personal transport on the public road network
- Parties involved in the provision of personal transport on the public road network
- Vehicle movement and harm causation
- Harm and Mitigation
- Product entity

To encourage the use of safety arguments, the following generic claim structures have been provided:

- Automotive personal transport service
- Vehicle lifecycle
- Vehicle lifecycle phase

In addition, possible claims for the different *vehicle* lifecycle phases have been given, see Table 7. The claims have a common format. There are claims about mitigations performed in the current phase, which mainly relate to staff and visitors; these are heavily based on non-technical solutions such as training and procedures. Then there are claims based on ensuring that all the necessary mitigation features are included in the design during the *development phase*. Examples of harm and design *mitigation measures* for each lifecycle phase are given in section 8, while section 9 lists typical topics that could be used to support development claims.

In section 6 the consequences of replacing the *human driver* by an *ADS* have been discussed.

Vehicle Phase	Claim	
Development	Dev_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* to manufacturing staff and plant visitors and, by its behaviour, to people encountered during its other lifecycle phases.
	Dev_Oth_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* to people encountered during its other lifecycle phases as a result of vehicle behaviour caused by the action, or inaction, of E/E systems.
Manufacturing	Man_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* to manufacturing staff and plant visitors and, by its behaviour, to people encountered during its other lifecycle phases.
	Man_Oth_1	All necessary information has been communicated to the development phase to allow appropriate design measures to be included in the design to enable the manufacturing plant to construct the *vehicle* without it causing *harm* to the staff and plant visitors and, by its behaviour, to people encountered during its other lifecycle phases
Pre-ownership	Pre-o_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* to people during its pre-ownership phase and, by its behaviour, to people encountered during the *in-use phase*
	Pre-o_Oth_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to enable pre-ownership activities without them causing harm to the staff and, by its behaviour, to people encountered during its other lifecycle phases
Pre-journey	Pre-j_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* to people during its *pre-journey phase* and, by its behaviour, to people encountered during the *journey phase*
	Pre-j_Oth_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to enable the *pre-journey* activities to be carried out without them causing harm to the staff and, by its behaviour, to people encountered during its other lifecycle phases.
During-journey	Dur-j_1	All appropriate measures have been taken to prevent the *vehicle* causing harm while in the *during-journey phase*.
	Dur-j_Oth_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to ensure no *harm* is caused by the vehicle during the vehicle journey
Post-journey	Post-j_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* while in the *post-journey phase.*
	Post-j_Oth_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to prevent *harm* to the *vehicle occupants* and *third parties* in the *post-journey phase* and, by its behaviour, to people encountered during its other lifecycle phases

Vehicle Phase	Claim	
Maintenance & Repair	M&R_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to prevent the *vehicle* causing *harm* to people during its *maintenance & repair phase* and, by its behaviour, to people encountered during the *in-use* and *decommissioning phases*
	M&R_Oth_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to prevent the *vehicle* causing *harm* to people during its *maintenance & repair phase* and, by its behaviour, to people encountered during the *in-use* and *decommissioning phases*
Decommissioning	Decom_1	All appropriate measures have been taken to prevent the *vehicle* causing *harm* to decommissioning staff and visitors
	Decom_Oth_1	All necessary information has been communicated to the *development phase* to allow appropriate design measures to be included in the design to ensure no *harm* is caused by the *vehicle's* behaviour during decommissioning

Table 7: Possible claims for the different vehicle lifecycle phases

8 Annex A - Examples by lifecycle phase

8.1 Development phase example

Example harm

Candidates for harm: Development staff.

Scenario: Unintended acceleration during closed track testing of prototypes, leading to *vehicle* collision with track infrastructure or other *vehicles*.

Example design measures for different control authorities

Human control authority

Design measures: Inclusion of powertrain emergency stop.

Human actions: Upon unintended acceleration, activate the emergency stop in the vehicle cabin (following operational procedures).

ADS actions: Not applicable.

Dependant roles: The vehicle manufacturer has a dependency on the human control authority to provide sufficient mitigation via the utilisation of the emergency stop feature. The assumption of the human actions should be documented in the operational procedures of the *vehicle manufacturer* (OB4.2.2).

ADS control authority

Design measures: Inclusion of powertrain emergency stop.

Human actions: Upon unintended acceleration, activate the emergency stop in the vehicle cabin (following operational procedures).

ADS actions: *ADS* can have the same access to request an emergency stop if it determines an unintended acceleration event.

Dependant roles: The vehicle manufacturer has a dependency on the *vehicle occupants* and the *ADS* to provide sufficient mitigation via the utilisation of the emergency stop feature. The assumption of the human actions should be documented in the operational procedures of the *vehicle manufacturer* (OB4.2.2).

8.2 Manufacturing example

Example harm

Candidates for harm: *Road users* (OB12)

Scenario: Unexpected *vehicle* behaviour during a journey (due to the installation of incorrect calibration software), leading to a *vehicle* collision with road infrastructure, other *vehicles* or *road users* (OB12)

Example design measures for different control authorities

Human control authority

Design measures: *Vehicle* configuration self-checks to prevent non-approved calibration data being installed, or preventing *vehicles* from operating with non-approved calibration data.

Human actions: To follow local operational procedures for the installation of correct calibration files.

ADS actions: Not applicable.

Dependant roles: The *vehicle manufacturer* has a dependency on the human manufacturing employee to follow procedures correctly.

ADS control authority

Design measures: *Vehicle* configuration self-checks to prevent non-approved calibration data being installed, or preventing *vehicles* from operating with non-approved calibration data.

Human actions: To follow local operational procedures for the installation of correct calibration files.

ADS actions: *Pre journey* check to ensure the *vehicle* does not report any calibration incompatibility faults.

Dependant roles: The *vehicle manufacturer* has a dependency on the human manufacturing employee to follow procedures correctly and the *ADS* to perform confirmation checks prior to starting a journey.

8.3 Pre-ownership example

Example harm

Candidates for harm: *Road users* (OB12).

Scenario: Unexpected vehicle behaviour during a journey (due to transport covers not being removed from camera systems), leading to a vehicle collision with road infrastructure, other vehicles or road users (OB12)

Example design measures for different control authorities

Human control authority

Design measures: Activation of certain *vehicle* features allowed only after diagnostic checks performed, including those for obscured camera systems

Human actions: PDI representatives to follow operational procedures.

ADS actions: Not applicable.

Dependant roles: The *vehicle manufacturer* has a dependency on the human PDI employee to follow procedures correctly.

ADS control authority

Design measures: Activation of certain *vehicle* features allowed only after diagnostic checks performed, including those for obscured camera systems

Human actions: PDI representatives to follow operational procedures.

ADS actions: *Pre journey* check to ensure the *vehicle* does not report any camera system faults including being obscured.

Dependant roles: The *vehicle manufacturer* has a dependency on the human PDI employee to follow procedures correctly and the *ADS* to perform confirmation checks prior to starting a journey.

8.4 Pre-journey example

Example harm

Candidates for harm: Persons performing *pre-journey* checks or completing actions from checks.

Scenario: Human performing under bonnet fluid checks / top up, with vehicle actuator movements allowed.

Example design measures for different control authorities

Human control authority

Design measures: Electronic Park Brake (EPB) interlock with bonnet open status, preventing driveaway.

Human actions: Set the *vehicle* in a benign state before performing *vehicle* checks.

ADS actions: Not applicable.

Dependant roles: The *vehicle manufacturer* has a dependency on the human control authority to provide sufficient mitigation. The assumption of the human actions should be documented in the *vehicle* owner's manual.

ADS control authority

Design measures: Provision for maintenance mode to disable automatic *vehicle* functions.

Human actions: Set *vehicle* in maintenance mode prior to under bonnet activities.

ADS actions: Prevent all actuator requests whilst in maintenance mode and do not exit maintenance mode without a human request.

Dependant roles: The *vehicle manufacturer* has a dependency on the *supply chain* (if providing the *ADS* control authority) for the *ADS* to behave as expected whilst 'maintenance mode' has been set. This requirement should be communicated to the *supply chain* and evidence of the confirmed behaviour recorded.

The *vehicle manufacturer* also has a dependency on the person performing the under-bonnet activities. The assumption of the human actions should also be documented in the *vehicle* owner's manual.

8.5 During journey example

Example harm

Candidates for harm: *Road users* (OB12)

Scenario: New road junction layout implemented by the local highways authority (*Government Departments* OB4.1.1), changing the allowed turning lanes from what was previously implemented. Leading to confusion and *vehicle* collisions.

Example design measures for different control authorities

Human control authority

Design measures: Not applicable.

Human actions: The human driver observes the signage and flow of traffic ahead, including near misses and confused behaviour. Approaches the junction based on the displayed signage information and with possible anticipation of other *vehicles* being out of position.

ADS actions: Not applicable.

Dependant roles: *Government Departments* (OB4.1.1) to provide standardised signage of the new layout as well as warning signage where significant changes have occurred.

Other Road Users (OB12) to be behaving in the same way as the human driver, adhering to signage and showing caution through the junction.

ADS control authority

Design measures: Ability to receive mandatory and secure over the air updates for the ADS.

Ability to report anomalies in expected and observed road layouts to *Engineering Developers and Manufacturers* (OB4.2)

Human actions: Not applicable.

ADS actions: Achieve the same level of controllability as a human driver, staying in the authorised lane and avoiding collisions with confused *Other Road Users* (OB12).

Observe and report anomalies in expected and observed road layouts

Dependant roles: *Government Departments* (OB4.1.1) to provide standardised signage of the new layout as well as warning signage where significant changes have occurred.

Government Departments (OB4.1.1) to provide details of future road changes to the *Engineering Developers and Manufacturers* (OB4.2).

Engineering Developers and Manufacturers (OB4.2) to incorporate the latest road infrastructure changes into the behaviour of new and deployed *ADS* prior to using the new road layout.

Engineering Developers and Manufacturers (OB4.2) to act on anomaly reports from the deployed *ADS*

Other *Road Users* (OB12) to be behaving in the same way as the human driver, adhering to signage and showing caution through the junction.

8.6 Post journey example

Example harm

Candidates for harm: *Road users* (OB12)

Scenario: Premature termination of a journey due to a *vehicle* issue, potentially leaving the *vehicle* and occupants as an obstacle in harms way. Likelihood of a collision with other *road users* (OB12) is high.

Example design measures for different control authorities

Human control authority

Design measures: Limp home or mechanical fall back of critical control systems, in order for the human control authority to move the *vehicle* to the safest position possible.

Human actions: Recognise that the *vehicle* has an issue and the journey needs to be terminated.

Manoeuvre the *vehicle* to a safe position on the side of the road.

Warn other *road users* of the stationary or slow moving *vehicle*.

Motorway driving - Vacate all passengers from the *vehicle* to a safe location behind the roadside barriers.

Contact breakdown and possibly emergency services.

ADS actions: Not applicable

Dependant roles: The *human driver* (OB4.3.1) must fulfil the actions defined above.

Breakdown services (included within OB4.6) to respond to the call out request.

Government departments (OB4.1.1) to specify suitably safe refuge for stranded *vehicles* and inform *road users* (OB12) of the obstacle through dynamic electronic signage.

Road builders and technology suppliers (OB4.2.1) to implement and maintain the specified refuge strategy and electronic signage.

ADS control authority

Design measures: Limp home or redundant critical control systems, in order for the *ADS* to control the *vehicle* to the safest position possible.

Include an *ADS* with the *behavioural competency* to recognise critical *vehicle* issues and to terminate the journey in a safe and controlled way as expected from a *human driver*.

Human actions: A fleet operator (part of OB4.6 *Companies operating and managing support services*) to contact breakdown and possibly emergency services as well as vacating all passengers from the *vehicle* to a safe location behind the roadside barriers.

ADS actions: Recognise that the *vehicle* has an issue and the journey needs to be terminated.

Manoeuvre the *vehicle* to a safe position on the side of the road.

Warn other *road users* of the stationary or slow moving vehicle. Placement of warning triangles could be a challenge here.

Dependant roles: The *ADS* must fulfil the actions defined above.

Breakdown services (included within OB4.6) to respond to the call out request.

Government departments (OB4.1.1) to specify suitably safe refuge for stranded vehicles and inform *road users* (OB12) of the obstacle through dynamic electronic signage.

Road builders and technology suppliers (OB4.2.1) to implement and maintain the specified refuge strategy and electronic signage.

8.7 Maintenance & repair example

Example harm

Candidates for harm: *Road users* (OB12)

Scenario: A forward facing radar sensor is replaced due to failure or damage without recalibration. Leading to undetected objects in the path of the *vehicle* and subsequent collisions.

Example design measures for different control authorities

Human control authority

Design measures: Automatic detection of uncalibrated sensors.

Prevention of the dependant Features being activated.

Indication to the *vehicle control authority* (OB20) of the unavailability of the associated Feature.

Prevention of *vehicle* drive away if necessary.

Human actions: The *human driver* should;

Observe the vehicle warnings of unavailable Features.

Assess and accept the risk of starting a journey.

Identify unwanted *vehicle behaviour* due to the uncalibrated sensor.

The repair technician should follow the repair procedures, as provided by the manufacturer, to replace and calibrate the sensor.

ADS actions: Not applicable.

Dependant roles: The *vehicle manufacturer* (OB4.2.2) to make the appropriate service instructions and tools available.

ADS control authority

Design measures: Automatic detection of uncalibrated sensors.

Prevention of the dependant Features being activated.

Indication to the *vehicle control authority* (OB20) of the unavailability of the associated Feature.

Prevention of *vehicle* drive away if necessary.

Human actions: The repair technician should follow the repair procedures, as provided by the manufacturer, to replace and calibrate the sensor.

ADS actions: Observe the *vehicle* warnings of unavailable Features.

To prevent the start of a journey with unavailable critical Features.

Identify unwanted *vehicle behaviour* due to the uncalibrated sensor.

Dependant roles: The *vehicle manufacturer* (OB4.2.2) to make the appropriate service instructions and tools available.

A fleet operator (part of OB4.6 *Companies operating and managing support services*) to assess and accept the risk of starting a journey.

8.8 Decommissioning example

Example harm

Candidates for harm: Decommissioning staff and visitors to the facility

Scenario: Partial disassembly of the *vehicle* with unexpected actuator movements, leading to a crushing or trapping event.

Example design measures for different control authorities

Human control authority

Design measures: Detection of a partially disassembled *vehicle* or crash event and deactivation of actuators.

Human actions: Staff to follow disassembly procedures to manually isolate all actuators before disassembly.

Staff to enforce physical boundaries between visitors and *vehicles* for disassembly.

ADS actions: Not applicable

Dependant roles: *Vehicle manufacturer* (OB4.2.2) to provide disassembly and isolation instructions, as well as the inherent monitoring and deactivation of actuators by the *vehicle* systems.

ADS control authority

Design measures: Detection of a partially disassembled *vehicle* or crash event and deactivation of actuators.

Human actions: Staff to follow disassembly procedures to manually isolate all actuators before disassembly.

Staff to enforce physical boundaries between visitors and *vehicles* for disassembly.

	A fleet operator (part of OB4.6 *Companies operating and managing support services*) to inform the ADS that it is in the decommissioning phase.
ADS actions:	To detect that the *vehicle* is in a decommissioning phase and prevent all actuator requests.
Dependant roles:	*Vehicle manufacturer* (OB4.2.2) to provide disassembly and isolation instructions, as well as the inherent monitoring and deactivation of actuators by the *vehicle* systems.

9 Annex B - Typical Topics to Support Development Claims

This annex lists Typical Topics that are mainly used to support development claims. IP indicates the phase in which the *mitigation measure* is implemented; MP indicates the phase in which the measure mitigates harm.

TE ID No	Topic	Evidence	IP	MP
TE01	The completeness of the knowledge of the infrastructure requirements	• Manual / automated survey of pre-defined route • Accumulated knowledge of infrastructure within ODD • Knowledge of planned infrastructure changes • Latest map data is accessed	*Dev*	*Dur-j*
TE02	The robustness of the autonomous control authority against the defined infrastructure	• Reports, analysis and mitigation of all unexpected behaviour during the journey, associated with the Road Infrastructure. (obtained during development) • Reports, analysis and mitigation of unexpected near misses/ accidents during the journey, associated with the Road Infrastructure. • Specification of intended infrastructure expected within the ODD	*Dev*	*Dur-j*
TE03	The robustness of the autonomous control authority against temporal changes to the intended route	• Vehicle reports of deficiencies in infrastructure • Test reports showing that the vehicle responds correctly when informed of official extreme weather warnings and road closure information • Test reports showing that the vehicle responds correctly when informed of latest traffic information	*Dev*	*Dur-j*
TE04	The robustness of the engineering of the base vehicle	• All applicable regulations have been met • All applicable standards have been met • Audit evidence of adherence to mature structured development process, with reviews and approvals	*Dev*	*Dur-j*

TE ID No	Topic	Evidence	IP	MP
TE05	The consistency of the behaviour of the vehicle and vehicle control authority	• Appropriate base vehicle attributes are proved to have been met with test reports, confirming that the base vehicle dynamic characteristics remain within the capability of the control authority • Simulation and vehicle test reports confirm that the automated control authority behaves consistently in all specified situations • Simulation and vehicle test reports confirm that the automated control authority monitors and acts on information during the journey to maintain safe and consistent vehicle performance	*Dev*	*Dur-j*
TE06	The completeness of the knowledge of the environment that the vehicle is intended to be deployed in	• Manual / automated survey of pre-defined route • Accumulated knowledge of infrastructure within ODD. • Use case environment reports	*Dev*	*Dur-j*
TE07	The assurance of correct vehicle configuration following maintenance / repair	• Published processes for configuration and calibration. • Development documentation for self checking of configuration & calibration	*Dev*	*M&R*
TE08	The assurance of correct field operation	• Field monitoring reports confirming intended behaviour	*Dev*	*Dur-j*
TE09	The completeness of information provided to owners and users	• Information provided to owners and users	*Dev*	*Pre-j*
TE10	The adequacy of the base vehicle performance, including its limits, for the intended purpose	• Base vehicle development data (E.g. design calculations, analysis, simulation and testing)	*Dev*	*Dur-j*
TE11	The knowledge and understanding of the vehicle control	• Vehicle performance limitation documentation, provided to the control authority	*Pre-j* *Dev (ADS)*	*Dur-j*

TE ID No	Topic	Evidence	IP	MP
	authority of the vehicle limits	• Vehicle control authority calibrated with base vehicle model		
TE12	The assurance of the correct use of the base vehicle controls	Receipt of base vehicle interface specification	*Dev*	*Dur-j*
TE13	The correctness of the interface between the vehicle control authority and the OEM vehicle platform controls	• Base vehicle development data ADS definition and development data • Data from ADS-equipped vehicle trials	*Dev*	*Dur-j*
TE14	The measures to address deficiencies previously identified by independent assessment	• Process to address deficiencies identified by independent bodies • Audit evidence of the process being used	*Dev*	*Dur-j*
TE15	The timeliness with which issues arising during operation are mitigated	• Field reporting process • Process for field data processing • Risk management process	*Dev*	*Dur-j*
TE16	The adequacy of the warnings and diagnostic information provided to the vehicle control authority	• Homologation results / certification • ADS definition and development data	*Dev*	*Dur-j*
TE17	The response of the vehicle control authority to all warning and diagnostic information	• ADS definition and development data	*Pre-j* *Dur-j*	*Dur-j*
TE18	The periodic updating of the vehicle to account for all official changes	• Process to discover official changes, E.g. map data, etc • Deployment process for vehicle updates • Evidence of periodic deployment	*Dev*	*Dur-j* *Pre-j*

TE ID No	Topic	Evidence	IP	MP
TE19	The ability of the vehicle manufacturer to prevent the start of new journeys in extreme circumstances	• Warning information provided in vehicle handbook • Design and verification evidence of base vehicle functions designed to prevent incorrect vehicle use • Design and verification evidence of ADS functions designed to prevent incorrect vehicle use	*Pre-j*	*Pre-j*
TE20	The ability of the vehicle manufacturer to prompt mandatory government checks or reduce availability of the vehicle	• Design and verification evidence of ADS functions designed to prompt mandatory government checks • Design and verification evidence of base vehicle functions designed to prompt mandatory government checks • Fleet operations process	*Dev* *Pre-j*	*Dur-j*
TE21	The roadworthiness of the vehicle prior to the start of a journey.	• Design and verification evidence of base vehicle functions designed to test key functions before vehicle use • Information about the recommended pre journey checks provided in the vehicle handbook • Design and verification evidence of ADS functions designed to test key functions before vehicle use	*Dev* *Pre-j*	*Dur-j*
TE22	The ability to check the roadworthiness of the vehicle prior to the start of a journey.	• Design and verification evidence of base vehicle properties facilitating roadworthiness checks prior to start of journey • Design and verification evidence of ADS properties facilitating roadworthiness checks prior to start of journey • Fleet operation process that incorporates vehicle roadworthiness checks	*Pre-j*	*Dur-j*

TE ID No	Topic	Evidence	IP	MP
TE23	The ability to monitor vehicle roadworthiness throughout the duration of the journey	• Design and verification evidence of base vehicle properties facilitating roadworthiness checks prior to start of journey • Design and verification evidence of ADS properties facilitating roadworthiness checks prior to start of journey • Fleet operation process that incorporates vehicle roadworthiness checks	*Dur-j*	*Dur-j*
TE24	The ability to monitor changes in vehicle performance throughout the duration of the journey	• Design and verification evidence of vehicle performance monitoring.	*Dur-j*	*Dur-j*
TE25	The response of the vehicle control authority to changes in vehicle performance	• ADS definition and development data	*Dur-j*	*Dur-j*
TE26	The ability to detect changes in vehicle noise, vibration, smell	• Design and verification evidence of sensing for vehicle secondary effects (vehicle noise, vibration, smell).	*Dur-j*	*Dur-j*
TE27	The adequacy of the Safety Policy to provide an appropriate level of safety	• Documented rationale for policies chosen	*Dev*	*Dur-j*
TE28	The implementation of the Safety Policy	• Design and verification evidence of vehicle behaviour reflecting Safety Policy	*Dev*	*Dur-j*
TE29	The maintenance and updating of the Safety Policy	• Process evidence for periodic updating of the Safety Policy based on operational experience • Periodic Safety Policy reviews	*Dev*	*Dur-j*

TE ID No	Topic	Evidence	IP	MP
TE30	The maintenance of consistent vehicle capability and suitability for use within the ODD	• Process for analysing in-field data • Process for discovering changes in the ODD • Periodic review reports of in-field data • Periodic review reports of ODD • Deployment process for vehicle updates • Evidence of periodic deployment	*Dev*	*Dur-j*
TE31	The timeliness of the updates made to the vehicle in response to field performance, road infrastructure changes, legal changes etc.	• Risk management process • Risk management review / meeting reports • Deployment process for vehicle updates • Evidence of periodic deployment	*Dev*	*Dur-j*
TE32	The vehicle control authority meets the driving performance criteria for its licenced usage	• Design and verification evidence of the vehicle behaviour in the ODD	*Dev (ADS)*	*Dur-j*
TE33	The ability to restrict the operation of the vehicle to regions where it is presently licensed	• Area of operation defined and documented • ADS definition and development data	*Dev*	*Dur-j*
TE34	The ability of the vehicle control authority to meet and maintain a pre defined driving ability	• Process for analysing in-field data • Periodic review reports of in-field data • Deployment process for vehicle updates • Evidence of periodic deployment	*Dev (ADS)*	*Dur-j*
TE35	The adequacy of the Safety Policy to incorporate all relevant ethical, legal and insurance / societal expectations	• Feedback from 3rd parties, both professional and general public	*Dev*	*Dur-j*
TE36	The communication of all vehicle control	• Conspicuity definition	*Dev*	*Dur-j*

TE ID No	Topic	Evidence	IP	MP
	authority intentions to other road users	• Design and verification evidence of vehicle control authority intention actuators		
TE37	The robustness of the vehicle control authority against deviant behaviour of other road users	• Studies of typical deviant behaviour in the ODD • Test plans • Design and verification evidence of the vehicle behaviour in the ODD	*Dev*	*Dur-j*
TE38	The consistency of the vehicle behaviour as perceived by other road users	• Study of key factors for assessing a situation for a mental model of current and future behaviour • Test plans • Design and verification evidence of the vehicle behaviour in the ODD	*Dev*	*Dur-j*

Table 8: Typical Topics to support development claims

10Terminology

The majority of terminology used is defined within the document. The following table defines additional key terms.

Term	Description
ACP	Assurance Claim Point
Harm	Physical injury or damage to the health of persons.
ODD	Operational Design Domain
Safety case	Argument that functional safety is achieved for items, or elements, and satisfied by evidence compiled from work products of activities during development.
System	Set of components or sub-components that relates at least a sensor, a controller and an actuator with one another.

11 References

[1] MISRA, Guidelines for Automotive Safety Arguments: HORIBA MIRA Limited, 2019.

[2] ISO 26262:2018, Road vehicles — Functional safety

[3] J. Birch, D. Blackburn, J. Botham, I. Habli, D. Higham, H. Monkhouse, et al., ”A Structured Argument for Assuring Safety of the Intended Functionality (SOTIF)” presented at the SafeComp, 2020. http://safecomp2020.di.fc.ul.pt/ (accessed 04/02/2024)

[4] R. S. Rivett, ”Public Road Transport System and Vehicle Models”, University of York 2022. https://www.york.ac.uk/assuring-autonomy/research/publications/public-road-transport-system-vehicle-models/ (accessed 04/02/2024)

[5] Ziebinski, R. Cupek, D. Grzechca, and L. Chruszczyk, ”Review of Advanced Driver Assistance Systems (ADAS)”, presented at the AIP Conference, 2017. https://pubs.aip.org/aip/acp/article-abstract/1906/1/120002/681133/Review-of-advanced-driver-assistance-systems-ADAS?redirectedFrom=fulltext (accessed 04/02/2024)

[6] MISRA, Safety assurance argument context for automated driving: 2024

[7] MISRA, Uncovering the historical road safety argument: 2025

[8] SysML Open Source Specification Project. Available: http://www.sysml.org/ (accessed 04/02/2024)

[9] SCSC-141C:2021, “Goal Structuring Notation Community Standard Version 3”, editor: Safety-Critical Systems Club C.I.C., 2021. Available: https://scsc.uk/scsc-141c (accessed 22/06/2026)

[10] UK Parliament (07/09/23). The Road Vehicles (Approval) Regulations 2020. Available: https://www.legislation.gov.uk/uksi/2020/818/made (accessed 04/02/2024)

[11] ISO 21448:2022 Road vehicles — Safety of the intended functionality

[12] ISO/SAE 21434 Road vehicles — Cybersecurity engineering

[13] SAE J3016:2021 “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles”

[14] ISO/TS 5083 Road vehicles — Safety for automated driving systems — Design, verification and validation. Under development

[15] User requirements to enable passengers of automated passenger services (APS) to perform journey tasks during emergencies: Department for Transport, 2025. Available: https://assets.publishing.service.gov.uk/media/68494325860362efc8e7883d/emergency-tasks-aps-research.pdf (accessed 13/3/26)

12 Revision history

Revision	Description of changes	Release date
Version 1.0	First version release	June 2026